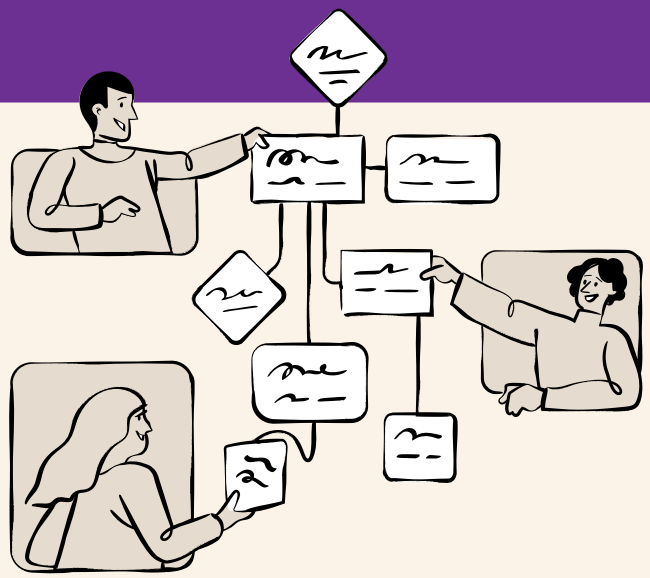
CT:IQ
Clinical Trials:
Thinking Smarter

Australian Research Data Commons

Responsibilities for the Secondary Sharing of Clinical Trial Data in Australia



Prepared by Dr James Scheibner, Lecturer in Law, Flinders University, Dr Lisa Eckstein, CT:IQ

Published by: CT:IQ
December 2025

TABLE OF CONTENTS

Australian Research Data Commons

This project has been funded by the Australian Research Data Commons

Acknowledgement of Country

CT:IQ acknowledges Aboriginal and Torres Strait Islander peoples as the traditional custodians of the land on which we meet, work and learn. We pay our respects to Elders past and present.

Advice to readers

The purpose of this work paper is to describe the ethical and legal responsibilities for the sharing of clinical trial data for secondary research in Australia. The work paper forms part of the broader ARDC/CT:IQ Project Clinical Research Data Sharing Frameworks. This work paper acts as a guide for data custodians, researchers and clinical trial sponsors who wish to use and disclose clinical trial data for secondary research purposes. Although specific responsibilities may need to be modified in certain cases, these are general principles which can be applied to a wide variety of research projects. The responsibilities are derived from a review of Australian legislation, regulations and guidelines, as well as a non-exhaustive search of regulatory documents. The work paper incorporates feedback received on an earlier draft version. The principles defined in this work package do not cover secondary uses that are not research. These secondary uses include but are not limited to clinical practice, quality improvement, training machine learning models or other statistical purposes.

Executive Summary

Scope

Increasingly, clinical trial data are being shared for secondary research (Hocking et al, 2019, p. iv). Sharing clinical trial data, including participant-level data, has numerous benefits. These benefits include improved verifiability and reproducibility of results, as well as more effective synthesis of evidence that reduces the need for further clinical trials (Hunter et al., 2024, p. 28; Thorogood and Knoppers, 2017, p. 58). In addition, sharing clinical trial data corresponds with the FAIR (Findable, Accessible, Interoperable, Reusable) principles, which encourage greater reuse of scientific data more broadly (Wilkinson et al., 2016). However, it is also important to ensure that secondary uses of clinical trial data are ethical and in compliance with relevant laws and guidelines. The purpose of this work paper is to synthesise legal and ethical responsibilities governing the secondary use of clinical trial data in Australia. It is anticipated that these responsibilities will be used as a general guide for data custodians, researchers and clinical trial sponsors.

There are no nationally or internationally agreed definitions for data management terms, however several organisations use specific definitions. For the purposes of this document, a definition of the terms used is provided in the data glossary included at Appendix 3: Data Glossary. The reader is advised that these definitions may differ from those used by other organisations.

This work paper has been developed to provide general information to the Australian research community. It should not be relied upon as legal advice. If you are unsure about your situation, please obtain legal advice.

The work paper reflects the law in Australia as of 30 September 2025. A detailed examination of how the principles of clinical trial data sharing apply in specific contexts is outside the scope of this work paper. In particular, this work paper recommends that Indigenous Data Governance requires special consideration but does not address the full details of those requirements.

Purpose of Writing

To synthesise legal and ethical responsibilities governing the secondary use of clinical trial data in Australia, this work paper involved two stages. The first was a comprehensive search for legislation and guidelines governing the secondary use of health data in Australia. This included Commonwealth, state and territory legislation as well as guidelines published by responsible agencies, including the Therapeutic Goods Administration of Australia (TGA), the National Health and Medical Research Council (NHMRC), the Australian Commission on Safety and

Quality in Health Care, and state, territory and local health agencies. The second stage involved a comprehensive but non-exhaustive search for guidance documents published on the secondary use of health data in Australia. This search included both guidance documents published by state and territory health agencies, as well as guidance documents with respect to specific data platforms.

Additional information on methodology is available in Appendix 1.

Key Principles for Sharing Clinical Trial Data

Based on the methodology used in this work paper, seven key principles have been identified as best practice to facilitate clinical trial data sharing. These are not intended to be in order of priority or a chronological sequence. Each of these principles might have greater importance for some research projects than others. However, they provide data custodians, researchers and clinical trial sponsors with guidance on what issues to consider with respect to the use of clinical data for future research.

1. **Establish clear, documented governance structures:** Determine the relevant actors in the governance of the clinical trial data. These include investigators, sponsors, data custodians and ethics review bodies, as well as institutions and researchers more broadly. The respective obligations of these actors should be documented in the data sharing policy of the study protocol (or similar).
2. **Define the data to be shared:** Assess whether the data in question could be defined as personal, re-identifiable or de-identified data. How data is classified will have an impact on how it can be used and disclosed.
3. **Confirm the scope of consent:** Confirm that the consent is adequate to enable the use of the data from a clinical trial dataset for future research purposes, and any need to obtain re-consent for use of that data.
4. **Optimise collection practices:** Consider how the clinical trial data has been collected from or generated about participants and accommodate these collection practices in sharing frameworks.
5. **Establish data management plans:** Develop a data management plan that applies to data custodians, researchers and sponsors.
6. **Share safely:** Implement documented procedures to assess requests for data sharing, including special considerations when on-sharing data or adding data to a repository. The obligations of secondary users of data should be documented using data sharing agreements.
7. **Engage with participants:** Incorporate community perspectives into data sharing arrangements, including Aboriginal and Torres Strait Islander peoples and individuals with rare diseases.

Part A. Legal and Ethical Requirements for Obtaining and Sharing Clinical Trial Data

The laws, including legislation, regulations and common law frameworks[1], that govern clinical trials can be classified into four categories: approval of clinical trials and data collection; consent for the use, collection and disclosure of clinical trial data; defining personal information; and storage and security while using and disclosing clinical trial data.

Approval of Clinical Trials and Data Collection

- Under the *Therapeutic Goods Act 1989* (Cth) s 19, clinical trials involving 'unapproved therapeutic goods' (as defined by the Act) must be conducted under either:
  - The Clinical Trial Notification (CTN) Scheme, which involves notification to the TGA along with review by an Australian Human Research Ethics Committee (HREC).
  - The Clinical Trial Approval (CTA) Scheme, which involves a product safety review by the TGA (Australian Clinical Trial Handbook: Guidance on Conducting Clinical Trials in Australia Using "Unapproved" Therapeutic Goods, 2021, pp. 18–22).
- The choice of scheme is to be made by the sponsor and confirmed by an HREC.
- If a clinical trial does not involve an unapproved therapeutic good, it does not need to proceed down either the CTN or CTA scheme. However, the trial will still require approval by an ethics review body (ERB) before it can commence (Australian Clinical Trial Handbook: Guidance on Conducting Clinical Trials in Australia Using "unapproved" Therapeutic Goods, 2021, p. 7).

Consent for the Collection, Use and Disclosure of Clinical Trial Data

- Consent for the collection, use and disclosure of personal or health information as part of a clinical trial is regulated under federal or state/territory privacy and/or health information legislation. The collection, use and disclosure of data must also be conducted in accordance with the NHMRC National Statement and Good Clinical Practice guidelines. Different privacy legislation applies depending on the legal status of the source of the clinical trial data.
  - If the entity that collected the data is a private institution or a Commonwealth government agency, federal data privacy laws will apply. These include the *Privacy Act 1988* and the *Healthcare Identifiers Act 2010*.

- If the entity that collected the data is a state or territory public institution, then local jurisdictional privacy and/or confidentiality provisions set out in health information management laws will apply. Some federal data privacy laws also bind state or territory agencies, such as the *Healthcare Identifiers Act 2010*. The applicable laws in each state and territory can be found here.
- Specific federal laws may also apply to certain data assets, which may include prohibitions on or requirements relevant to sharing. The *My Health Records Act 2012* and associated regulations apply to Australia's summary health care record system My Health Record. The *National Health Act 1953* and associated rules apply to the Pharmaceutical Benefits Scheme and data collected as part of this scheme. The *Health Insurance Act 1973* applies to data collected as part of the Medicare Benefits Schedule. Although these laws do not apply to participant-level data in clinical trial datasets, certain research projects may seek to link clinical trial data with these data assets.
- There may be other laws which apply depending on the nature of the research and which are listed by jurisdiction in **Appendix 2 Table 1**:
  - Public health legislation will apply to health information that is collected by a state health department for public health research or quality improvement purposes.
  - Mental health legislation will apply to research involving information collected as part of a mental health service

- Privacy or health information legislation provides a pathway for the use and disclosure of health information for research purposes either with the consent of the participant or, if no consent is available, if a waiver of the requirement for consent has been approved by an ERB and no other legal obligations would prevent sharing.
- The ERB can also determine whether an opt out approach or a waiver of the requirement for consent (as opposed to opt in consent) is appropriate for the project. Only an HREC can approve a waiver of the requirement for consent for research seeking the use or disclosure of personal information in medical research, or personal health information, or for a clinical trial conducted under the CTN or CTA Scheme.
- Even if an ERB is satisfied that a waiver of the requirement for consent should be granted, there may be other legal and ethical duties which may operate against using or disclosing the data without consent. For example, data shared between a patient and their general practitioner may be subject to the common law duty of confidentiality (Adams et al., 2025). The sharing of this data may also constitute a breach of the statutory tort for serious invasions of privacy in Schedule 2 of the *Privacy Act 1988*.

Consent for involvement in a clinical trial for individuals who lack capacity is primarily covered under state and territory legislation. The involvement of adults with impaired capacity is covered under guardianship and administration

legislation whereas consent for children is covered under common law principles, as well as consent to medical treatment legislation in New South Wales and South Australia. A list of this legislation is contained in **Appendix 2, Tables 1 and 2.**

Guidelines published by the NHMRC interact with relevant privacy laws to allow certain health and medical research to be done without consent. These guidelines include the National Statement on Ethical Conduct in Human Research, as well as the guidelines approved under sections 95 and 95A of the *Privacy Act 1988*. However, these guidelines should be read in conjunction with and limited by other legal obligations such as the duty of confidentiality.

The Section 95 guidelines apply to medical research where personal information held by a government agency needs to be used without consent. These guidelines define what researchers need to supply to a HREC when seeking to access personal information for medical research without consent (Guidelines Under Section 95 of the *Privacy Act 1988*, 2024, para. 2.1 to 2.7).

The Section 95A guidelines apply to collecting, using or disclosing health information held by private sector organisations for research relevant to public health or safety (Guidelines Approved under Section 95A of the *Privacy Act 1988*, 2024, para. A1.1). The Section 95A guidelines also apply to private sector organisations which collect and use health information to compile or analyse statistics for public health or public safety purposes (Guidelines Approved under Section 95A of the *Privacy Act 1988*, 2024, para. B1.1). Further, the Section 95A Guidelines apply to private sector organisations that collect and use health information to manage a health service (Guidelines Approved under Section 95A of the *Privacy Act 1988*, 2024, para. C1.1). The principles of Free, Prior and Informed Consent which are discussed in Part 7. Engage with Participant Groups will also apply to research involving Aboriginal and Torres Strait Islander peoples and communities. The Free, Prior and Informed Consent principles allow Aboriginal and Torres Strait Islander research participants to modify or withdraw their consent to participate in research at any time.

Defining Personal Information

Under Commonwealth and Australian Capital Territory legislation, ‘personal information’ includes any information about a person who is identifiable or is reasonably identifiable (*Privacy Act 1988* (Cth), s 6; *Information Privacy Act 2014* (ACT), s 8(1)). Under other state and territory legislation, personal information includes any information or opinion about an individual who is identifiable or whose identity can be reasonably ascertained (*Privacy and Personal Information Act 1998* (NSW), s 4(1); *Information Act 2002* (NT), s 4A(1); Information Privacy Act 2009 (QLD), s 12; *Personal Information Protection Act 2004* (TAS), s 3, *Privacy and Responsible Information Sharing Act 2024* (WA), s 4). This definition is also used in state and territory data governance documents (National Health Information Standards and Statistics Committee, 2017, p. 3; NT Health Data

Release Guidelines, 2018, p. 20; Research Governance Procedures, 2021, p. 50). Unless future case law determines otherwise, it can be assumed that both definitions are equivalent.

Commonwealth, state and territory privacy and health information management legislation also applies to 'health information'. This definition can encompass information about the health of an individual or health services provided to an individual. It can also encompass personal information collected whilst providing a health service, as well as genetic information (*Privacy Act 1988* (Cth), ss 6(1) and 6FA; *National Health Act 1953* (Cth), s 135AC(1); *Health Insurance Act 1973* (Cth), s 129AAD; *Health Records (Privacy and Access) Act 1997* (ACT), Dictionary (definition of 'health information'); *Health Records and Information Privacy Act 2002* (NSW), s 6; *Information Act 2002* (NT), s 4; *Information Privacy Act 2009* (QLD), sch 5 (definition of 'health information'); *Personal Information Protection Act 2004* (TAS), s 3; *Health Records Act 2001* (VIC), s 3; *Privacy and Responsible Information Sharing Act 2024* (WA), s 4). This definition is used across Commonwealth, state and territory guidelines (National Health Information Standards and Statistics Committee, 2017, p. 17).

The scope of public health laws varies more noticeably between different states and territories. New South Wales, Northern Territory and Victorian public health laws cross reference privacy or health information management laws (*Public Health Act 2010* (NSW), s 98; *Public and Environmental Health Act 2011* (NT), s 4; *Public Health and Wellbeing Act 2008* (VIC), s 3). South Australian and Tasmanian public health laws create their own definition of personal information (*Public Health Act 2011* (SA), s 99(4); *Public Health Act 1997* (TAS), s 3). Queensland and Western Australian public health laws apply to 'confidential information' and 'specified information' respectively (*Public Health Act 2005* (QLD), ss 219, 228H, 237, 279AK; *Hospital and Health Boards Act 2011* (QLD), s 142; *Public Health Act 2016* (WA), s 298). Therefore, before requesting information for research or a clinical trial, a researcher or sponsor should determine if one or more of these laws apply to that information. Further, approval may need to be sought from a particular agency before this confidential information can be used. For example, in Queensland, a decision maker within the Department of Health needs to authorise access to confidential information for research purposes held by the Department (Hospital and Health Boards Act 2011 (QLD), s 150A; *Public Health Act 2005* (QLD), ss 281-292).

Likewise, mental health laws govern information about the delivery of mental health services. These laws vary between different states and territories. The Western Australian Department of Health may request that a mental health service disclose relevant information for research purposes. This relevant information can include information about the treatment or care of a person, as well as information relevant for the planning of mental health services or epidemiological analysis and research into mental health (*Mental Health Act 2014* (WA), s 572(3)). Similarly, in the Northern Territory and South Australia, information about an individual's mental health treatment can be disclosed for

research purposes (*Mental Health and Related Services Act 1998* (NT), s 91(2)(j); *Mental Health Act 2009* (SA), s 106(2)(f)). Other legislation, such as in New South Wales, Queensland, Tasmania and Victoria, cross references equivalent state privacy laws with respect to when data can be used for research purposes (*Mental Health Act 2007* (NSW), s 189(1)(d1); *Mental Health Act 2016* (NSW), s 778(3)(b); *Mental Health Act 2013* (TAS), s 134 (1)(b); *Mental Health and Wellbeing Act 2022* (VIC), s 671(3)).

Storage and Security of Clinical Trial Data

Depending on the data custodian or sponsor responsible for holding a dataset, either Commonwealth or state and territory legislation—along with the applicable consent collected and contracts governing the dataset—will apply to storage and sharing practices. This legislation includes privacy and health information legislation, as well as legislation governing public documents. A list of this legislation is provided in **Appendix 2 Table 3**.

According to the NHRMC Management of Data and Information in Research guide, how long data needs to be retained depends on the purpose of the research project with which it is associated. For most research projects, data must be retained for at least 5 years from the date of publication. For clinical trials, data should be retained for a minimum of 15 years. For genomic research, the data may need to be retained indefinitely (National Health and Medical Research Council, 2019, p. 3). In addition, there are state and territory guidelines which apply to the storing and security of records by public sector agencies, including clinical trial data and associated documents. These guidelines are contained in **Appendix 2, Tables 3 and 4**.

Further, there may be other legal obligations that govern how data can be stored and shared. For example, the data sharing agreement governing the dataset may specify the data custodian does not own or hold the data. In these cases, the data custodian will need to seek approval from the entity specified in the data sharing agreement. Additionally, funding bodies may place obligations on the recipient of a grant regarding how data may be stored and used. If these obligations do not support secondary use, approval may need to be sought from the funding body.

Part B. Principles for Sharing Clinical Trial Data

The following seven key principles were identified as best practice to facilitate clinical trial data sharing. These are not intended to be in order of priority or a chronological sequence. Each of these principles might have greater importance for some research projects than others. However, they provide data custodians, researchers and clinical trial sponsors with guidance on what issues to consider with respect to the secondary use of clinical data.

1. Establish clear, documented governance structures

A foundation for responsible data sharing is the availability of clear governance structures, including roles and responsibilities for data management and sharing decisions. This generally will involve some or all the items below. The data governance structures should be recorded in relevant documentation, including the study protocol, data sharing policy, clinical trial research agreements and/or other relevant trial documentation.

a) Data Custodians, Data Access Committees and Data Stewards

A 'data custodian' is any entity, including an organisation, agency or person, responsible for managing the use, disclosure and protection of data in a dataset (Principles for Accessing and Using Publicly Funded Data for Health Research, 2016, p. 12). The data custodian may also be responsible for ensuring that the dataset adheres to quality and security standards (NT Health Data Release Guidelines, 2018, p. 18; Rowlands et al., 2024, p. 19). Two or more entities may be joint data custodians if they are jointly responsible for the quality and security of the dataset. If an entity such as a research organisation requests access to a dataset, all data custodians should approve access to that dataset, depending on what is specified in the data sharing agreement (National Health Information Standards and Statistics Committee, 2017, p. 4).

In some cases, it may be unclear who is responsible for maintaining and reviewing information in a dataset. For example, a government agency may collect clinical trial data and then store this data on a third-party cloud computing provider. In these circumstances, it is unclear whether the data custodian is the agency (which is responsible for collecting the data), or the cloud computing provider. Therefore, the entity which is 'data custodian' should be determined via contract or legal agreement (Moses, 2020, p. 630; Krebs and Moses, 2024, p. 135). Doing so will ensure that responsibility and accountability for the use of data is clear (Adams et al., 2022a, p. 225).

The terms 'data access committees' and 'data steward' are sometimes used synonymously with 'data custodian' and these entities may operate in a similar manner. Depending on the size of the dataset, a data access committee may be

appointed to oversee the overall strategy associated with the dataset (NT Health associated with the dataset (NT Health Data Release Guidelines, 2018, p. 11). These objectives will depend on the overall nature of the project. However, they could include assessing applications to access the data, considering the need for ethics approval, supervising linkage or de-identification, assessing risk and conducting monitoring activities (Framework to Guide the Secondary Use of My Health Record System Data, 2018, p. 9).

b) HRECs and Other Ethics Review Bodies

Human Research Ethics Committees (HRECs) are specialised committees that protect the welfare and rights of participants in research. HRECs are responsible for ensuring that research proposals are ethically acceptable and that research participants are protected in research protocols, including for clinical trials. Institutions may establish non-HREC ethics review bodies (ERBs) for the ethics review of lower-risk research (National Statement para 5.1.12).

HRECs and ERBs do not have overarching responsibility for research governance or dataset strategy. These decisions should be determined by a data custodian, data access committee or a data steward. HRECs should instead focus on whether the benefits of the proposed research outweigh any potential risks and whether participants are treated with respect, (Adams et al., 2022a, pp. 225–226) noting that this may require assurances to the HREC of suitable governance and/or access arrangements.

Approval by an ERB is a necessary but insufficient step for sharing decisions. A data custodian should make the final decision on whether to approve access to the data based on the trial's Data Sharing Policy and other relevant considerations. Therefore, even if an ERB has approved access to a dataset, the data steward or stewards may refuse access (Guidelines Under Section 95 of the Privacy Act 1988, 2024, para. A1.6, B1.6 and C.16).

c) Data Sharing Agreements

Before any external researcher or sponsor uses a dataset from a clinical trial for secondary purposes, the data custodian should ensure that there is a data sharing agreement in place. Data sharing agreements are different from data sharing policies because agreements only apply to the parties in a particular project. Data sharing agreements are also contracts and therefore are legally binding on the parties to the agreement. Any data sharing agreement templates should be approved by the data custodian.

The contents of the data sharing agreement will depend on the data being accessed (Research Governance Procedures, 2021, p. 14). However, the agreement should contain at minimum three key provisions:

1. The data sharing agreement should specify the terms on which a secondary research project can access the clinical trial data, and that data cannot be used for a purpose not covered under the agreement. The agreement should also specify the data that is being shared and the consents that have been obtained for the use of that data. For example, if extended or unspecified consent has only been obtained for a subset of participant-level data in a dataset, only that subset can be transferred subject to the agreement.
2. The data sharing agreement should specify the privacy and security obligations of the person or entity accessing the clinical trial data, including how the dataset can be accessed and by who. The agreement should also prohibit any unauthorised re-identification of any individuals from participant-level data.
3. Any data breach or loss should be reported to the responsible regulator/s, as well as any participants who are included in the dataset. The responsible regulator/s could include the Office of the Australian Information Commissioner or state and territory information privacy commissioner, depending on the identity of the data custodian (Framework to Guide the Secondary Use of My Health Record System Data, 2018, p. 61).

The study protocol, clinical trial research agreement, and/or data sharing policy should document the provisions that are required or recommended for inclusion in data sharing agreements.

2. Define the data to be shared

Responsible data sharing requires managing the privacy and confidentiality risk to which participants are exposed by third parties accessing participant-level data. This process requires assessing both the likelihood of a potential risk to privacy or confidentiality, as well as the magnitude of that risk. How data, and the risk associated with data, is classified will impact the legal and ethical parameters for use and disclosure.

As explained in Part A, federal and state and territory legislation define whether information should be considered ‘personal information’ for the purposes of Australian privacy laws. These definitions provide a key step for characterising the information in given clinical trial datasets and associated responsibilities. Under this category-based model, data that falls outside the definition of ‘personal information’ is considered to present little to no privacy risk and generally falls outside the scope of legislative requirements.

However, the National Statement on Ethical Conduct in Research Involving Humans has moved away from a category-based model to explicitly recognise that the identifiability of information, and thus the privacy risk to participants, exists on a continuum. Most notably, it states that “Due to technological advances, risks may arise in relation to data and/or information that has never been labelled with individual identifiers or from which identifiers have been permanently removed” (National Statement on Ethical Conduct in Human

Research, 2025, p. 33). Further, recent decisions of the Office of the Australian Information Commissioner have confirmed this interpretation of a continuum of identifiability (*Commissioner initiated investigation into Clearview AI Inc. (Privacy)* [2021] AICmr 54, [96]; Clearview AI Inc and Australian Information Commissioner [2023] AATA 1069, [109-111]; *Commissioner Initiated Investigation into the Australian Federal Policy (Privacy)* [2021] AICmr 74). However, the Commissioner has observed that an individual will be not reasonably identifiable from a dataset if reidentification is excessively time-consuming or costly in the circumstances (Kind, 2025).

While defining clinical trial data in accordance with the below categories remains crucial for understanding legal and regulatory responsibilities, a continuum-based approach may supersede category-based approaches in future legislation. Therefore, this approach should be adopted with respect to data collected as part of a clinical trial.

a) Personal information

Personal information includes individually identifiable information or opinions and —in some instances—other participant-level data.

Individually identifiable information is information which can be used to directly identify an individual. This could include, for example, names, addresses, postcodes, full dates of birth or unique personal identifiers such as Medicare numbers (NT Health Data Release Guidelines, 2018, p. 20). In some states (such as New South Wales), this definition includes information about deceased individuals (*Privacy and Personal Information Protection Act 1998* (NSW) s 5(3)(a), which specifies the provisions apply to persons who have been dead for 30 years or less). Datasets could also contain individually identifiable data where there is only a small number of records with the same data attribute; for example, a rare medical diagnosis (Data Access and Release Policy, 2023, p. 14). Individually identifiable information will constitute personal information for the purposes of privacy laws.

A dataset will contain ***participant-level data*** (otherwise known as patient-level data, individual participant data, microdata or unit-level data) when it contains information about individuals or individual records. This data could include observations for an individual or an organisation, such as responses to a survey or an administrative form (National Health Information Standards and Statistics Committee, 2017, p. 18). Participant-level data is not necessarily identifiable information or personal information for the purposes of privacy laws, but there is a greater risk of re-identification than with aggregate or non-identifiable data (NT Health Data Release Guidelines, 2018, p. 20). This risk will depend on the number of identifiers and quasi-identifiers attached to the data, as well as the associated data governance practices. This risk is becoming more acute with the use of artificial intelligence tools to link seemingly deidentified datasets.

b) Non-Identifiable, Re-Identifiable and Aggregate Data

Non-identifiable (sometimes referred to as ***de-identified data***) refers to data that has never been labelled with individual identifiers, where identifiers have been permanently removed, or where identifiers have no meaning to recipients (National Health Information Standards and Statistics Committee, 2017, p. 17).

- *Non-identifiable data*: When data has been rendered non-identifiable, it is highly unlikely without legal or technical means to re-identify individuals or individual records without excessive or time-consuming effort (NT Health Data Release Guidelines, 2018, pp. 18–19; Kind, 2025).
- *Re-identifiable data*: Where individual identifiers have been replaced with a code or a pseudonym. Individuals in the dataset can be re-identified using the code. Alternatively, individuals in the dataset can be re-identified if the dataset is combined with another dataset (National Health Information Standards and Statistics Committee, 2017, p. 18).

Data can also be rendered non-identifiable by aggregating the data. For example, instead of publishing the age of each participant, a journal article might publish how many people in a dataset are of a particular age or age range (National Health Information Standards and Statistics Committee, 2017, p. 18).

Non-identifiable data and aggregate data will not usually meet the definition of 'personal information' for the purposes of Australian privacy laws. However, re-identifiable data can satisfy the definition of personal information (Adams et al., 2025, p. 847-8). Likewise, the National Statement states that the identifiability of personal information exists on a continuum, rather than being a binary characteristic (National Statement on Ethical Conduct in Human Research, 2023, p. 33). Further, the more values associated with each record in a dataset, the more likely these values could become quasi-identifiers to divide a dataset into smaller strata (Rodriguez et al., 2025, p. 3)

Therefore, datasets should be presumed to contain identifiable data unless established otherwise, and robust data governance frameworks are used to control access to those datasets, alongside the application of de-identification techniques where appropriate (National Health Information Standards and Statistics Committee, 2017, p. 5; Kind, 2025). Whether or not a dataset still contains identifiable data depends on the circumstances in which that data is used and analysed. As discussed previously, a person will not be identifiable if in the circumstances it would be excessively or time-consuming to re-identify them from de-identified data (Kind, 2025).

c) Techniques to minimise re-identification and disclosure risks

Before sharing clinical trial data for secondary research, data custodians should consider several steps to reduce the risks of re-identification and disclosure.

1. The data custodian should remove or modify any personal identifiers in the dataset. If a researcher or sponsor needs to know that multiple records relate to a single participant, these identifiers should be replaced with a pseudonym (National Health Information Standards and Statistics Committee, 2017, pp. 5, 8).However, by itself this approach will usually not be enough to render the data de-identified and may need to be coupled with other organisational measures (Kind, 2025).
2. Unless the precise values of participant level data are required for a research project, the data custodian should consider applying privacy-preserving techniques. For example, dates of birth could be replaced with 5-year age groups, or postcodes could be replaced with a metropolitan/rural category (National Health Information Standards and Statistics Committee, 2017, p. 5). Similarly, the exact date of a hospital admission could be replaced with the month and year of admission.
3. The data custodian should consider suppressing small cell sizes for all releases of data, including aggregate data. Records can be suppressed by grouping values together (National Health Information Standards and Statistics Committee, 2017, pp. 6–7).

There is no one technique that can be used to prevent re-identification and different techniques may impact the validity of data. Instead, data custodians should judge which techniques are most appropriate to minimise the risk that individuals in a dataset will be re-identified. A person with expertise in de-identification may be appointed to choose or oversee these techniques if there is no appropriate expertise in a research team (Framework to Guide the Secondary Use of My Health Record System Data, 2018, p. 39). Ultimately, a dataset will no longer contain personal information when individuals or individual records are no longer reasonably identifiable from that dataset (Kind, 2025). The United States National Institute of Standards and Technology (NIST) has provided a list of techniques that can be used to de-identify government datasets. Depending on the clinical trial, some or all these techniques may be applicable to clinical trial datasets (Garfinkel et al., 2023).

3. Confirm the scope of consent

Clinical trial data sharing can help improve the quality and transparency of scientific research, as well as reduce the cost of future clinical trials (Modi et al., 2023, pp. 400). However, it is also important to respect the wishes of participants who are enrolled in clinical trials and whose individual participant data may be shared (Principles for Accessing and Using Publicly Funded Data for Health Research, 2016). Therefore, trials should plan from the outset of how they will govern and manage data sharing. This planning should include how researchers will seek participant consent to sharing data. Express consent obtained at the time of the trial is the most ethically and legally robust framework for future sharing. While mechanisms exist for sharing data for secondary research without consent in some circumstances (e.g. if a waiver of the requirement for consent is provided), these should be relied upon only as a final option. There may also be other legal and ethical duties which militate against the sharing of data via a waiver without consent. These include the duty of confidentiality and the terms of data sharing agreements (Adams et al., 2025, p. 853).

a) Fundamental principles of consent

Ideally, data custodians should only collect sensitive personal information for research purposes with consent (*Privacy Act 1988* (Cth), sch 1 pt 2 cl 3.3(a)) However, sometimes obtaining consent may not be possible. For example, individuals may die or lose capacity in between contributing their data to a dataset and the establishment of a research project. If consent has not been obtained, or if the requirements for a valid consent have not been satisfied, then a new consent must be obtained from a valid decision-maker (for example, a next of kin as authorised under applicable guardianship laws) or a waiver of the requirement for consent must be obtained for the use of information in research.

There are four key requirements for valid consent which apply to all forms of consent described in this section:

1. A person must give consent voluntarily. That means they must have sufficient time to understand the proposed request, ask further questions, and seek advice. Consent is not voluntary if a person cannot freely refuse to consent. Consent is also not voluntary if a person needs to consent to receive a government service.
2. A person must be given clear information about how their data will be used when their consent is sought, as well as how long their consent will be valid.
3. A person must give as specific a consent as possible to the use of their data, including the types of information being collected and disclosed.
4. An individual must communicate their consent, for example, by signing a physical or digital form, click a button or state that they consent during a recording (Fact Sheet - Consent, 2023).

Adults are presumed to have capacity to consent. At common law and under the laws of most Australian states and territories, an adult is any person who is 18 years or older. However, some state legislation sets a different age for capacity to make health care and data sharing decisions. For example, in South Australia, a person will have capacity to consent to medical treatment (including research and involvement in clinical trials) if they are 16 years or older (*Consent to Medical Treatment and Palliative Care Act 1995* (SA), s 4(1), s 12).

If a person has a physical or mental disability, or is suffering from temporary incapacity, their capacity may be impaired. If a person has impaired capacity, someone else will need to consent on their behalf to be involved in a research project or clinical trial. This person could include a legal guardian, a person responsible for the care of the participant or the family member (*Guide - Privacy and Persons with Reduced Decision-Making Capacity*, 2021).

In addition, under Australian privacy law a participant is usually entitled to access their personal information and have it corrected once it has been collected by an APP entity or state government agency (*Privacy Act 1988* (Cth), sch 1, pt 4, cls 12.1, cls 13.1; *Information Privacy Act 2014* (ACT), sch 1, pt 1.5, cls 12-13; *Health Records (Privacy and Access) Act 1997* (ACT), s 10(1), *Privacy and Personal Information Protection Act 1998* (NSW), ss 14-15; *Health Records and Information Privacy Act 2002* (NSW), sch 1 cls 6-7; *Information Act 2002* (NT), sch 2 cl 6.1; *Information Privacy Act 2009* (QLD), sch 3 pt 5 cls 12.1, 13.1; *Personal Information Protection Act 2004* (TAS), sch 1 cl 6; *Privacy and Data Protection Act 2014* (VIC), sch 1 cls 6.1, 6.6; *Health Records Act 2001* (VIC), sch 1 cls 6.1, 6.5; *Privacy and Responsible Information Sharing Bill 2024* (WA), sch 1 cl 6.1, 6.5).

Whether this right of access and correction is available may be unclear when dealing with personal information collected as part of a clinical trial. Private sector organisations do not need to grant access to personal information, including health information, if it would be a risk to public health *(Privacy Act 1988* (Cth), sch 1, pt 4, cl 12.3(a)). However, no such right of refusal exists under health privacy law in the ACT, New South Wales and Victoria. With respect to the right of correction, private sector organisations can refuse to correct personal information except to the extent it would be unreasonable *(Privacy Act 1988* (Cth), sch 1, pt 4, cl 13.3(a); *Health Records (Privacy and Access) Act 1997* (ACT), sch 1, cl 7.3; Health Records and Information Privacy Act 2002 (NSW), sch 1, cl 8(2); *Health Records Act 2001* (VIC), sch 1, cls 6.6-6.9). A further complicating factor is that the Good Clinical Practice guidelines are silent as to whether a patient has a right to access and correct their health care records. Instead, the guidelines only mention that regulatory authorities, the monitors and auditors of clinical trials and ethics review bodies should have direct access to records (ICH Guideline for Good Clinical Practice, 2022, Sections 1.21, 4.8.10(n), 5.15, 6.10). Further, sponsors only have access to pseudonymised or coded participant information and cannot re-identify subjects (ICH Guideline for Good Clinical Practice, 2022, Sections 1.58 and 5.5.5, Lalova-Spinks et al., 2022, p. 15).

A participant should also be given the opportunity to refuse their data being used for secondary purposes (Framework to Guide the Secondary Use of My Health Record System Data, 2018, p. 19). This opportunity should be provided without any consequences to the participant should they seek to rely on it. Unlike the right to access and correct their medical records, a patient's right to withdraw from a clinical trial is explicitly protected by the Good Clinical Practice guidelines (ICH Guideline for Good Clinical Practice, 2022, Section 4.8.10(m)). However, clinical trial sponsors also need to maintain appropriate data quality to ensure that data are reliable and have been processed correctly (ICH Guideline for Good Clinical Practice, 2022, Section 5.1.3). This requirement may clash with a participant's right to withdraw from a trial, particularly if data processing has begun. Further, the Good Clinical Practice guidelines require clinical trials to be scientifically sound (ICH Guideline for Good Clinical Practice, 2022, Section 2.5). If an individual seeks to withdraw from a clinical trial and have their data erased if they experience an adverse event, it could mean that important safety information is no longer available in the final findings of the trial (Data Retention When Subjects Withdraw from FDA-Regulated Clinical Trials, 2008, p. 7). Another complicating factor is that there is no right to erasure that is currently present in Australian privacy law at either the Federal or state and territory level (Privacy Act Review Report 2023, p. 18, 30; Krebs and Moses, 2024, p. 114).

Therefore, it is ultimately up to the research team to appropriately define the right of participants to access, correct and withdraw their data into the participant information consent form (PICF), unless there are legal requirements which specify otherwise (such as record keeping requirements specified in Appendix 2 Tables 3 and 4). The PICF must balance participants being able to exercise their rights under privacy legislation against ensuring the quality of clinical trial data. The PICF should specify who participants should contact if they wish to access their records (Lalova-Spinks et al., 2022, p. 15). Further, the PICF should explicitly specify that even if a participant withdraws from a trial, their data may need to be retained to ensure data quality and scientific validity of the trial. Finally, for both prospective clinical trials as well as clinical trials where data has already been collected, it is important to build an ongoing relationship of trust with participants. Being open and transparent with participants about how their data is being used can help participants do not feel the need they need to withdraw from a study or correct their data (Laurie & Postan, 2013, p. 413).

There may be situations where data custodians or researchers may make exceptions to this rule. For example, if data from Indigenous research participants is used or generated as part of a clinical trial, those participants should have a mechanism to correct or withdraw their data.

b) Alternatives to Specific Consent

Traditionally, consent has been conceptualised as an authorisation for each specific sharing activity. However, modern data sharing practices often seek to rely upon a single consent to authorise multiple data sharing activities. This practice warrants careful attention and legal and ERB advice to ensure relevant requirements have been satisfied.

i) Bundled consent
Bundled consent involves seeking a single consent from an individual to use or disclose their data for multiple different purposes. If bundled consent is sought from an individual, they should be provided sufficient information on all intended purposes. Since an individual cannot refuse to consent to specific intended purposes with bundled consent, bundled consent should only be sought for the necessary intended purposes (Fact Sheet - Consent, 2023).

(ii) Unspecified consent
Unspecified or broad consent allows data to be used or disclosed for any future research project subject to specified imitations (e.g., future approval by an ERB or HREC) (Eckstein et al., 2023, p. 507). The gravity of the consequences of unspecified consent should be reinforced to the individual at the point that a participant provides consent to a clinical trial (National Statement on Ethical Conduct in Human Research, 2023, para. 2.2.14-2.2.16; Otlowski, 2012, p. 208).

(iii) Extended consent
Extended consent allows data to be used or disclosed for future research projects that are related to an existing project. Extended consent may also allow clinical trial data to be used or disclosed for future research in the same field as the original trial. Extended consent is not as comprehensive as broad consent, but it is preferable to obtain explicit extended consent (Eckstein et al., 2023, p. 507; National Statement on Ethical Conduct in Human Research, 2023, para. 2.2.14-2.2.15).

(iv) Dynamic consent
Dynamic consent provides a flexible approach for providing participants with digital tools to control the way in which their data is used (Teare et al., 2021). This allows participants to select different types of consent structures for future research use of samples and data, including specific, unspecified and extended consent. The technologies by which dynamic consent is implemented provides opportunities for participants to review and update these consent preferences over time (Researcher User Guide, 2023, pp. 37–38). However, at the time of writing, researchers in Australia are only rarely using dynamic consent platforms (Haas et al., 2024; Teare et al., 2021). The use of dynamic consent may increase once more platforms become available or existing platforms are developed to support a broader part of the research sector.

c) Sharing without adequate consent

For some clinical trials, sponsors and researchers may seek to share trial data in the absence of clear or specific participant consent. However, under privacy and health information law, whether a data custodian or researcher can share clinical trial data depends on the scope of consent at the time of data collection. If the scope of the consent provided is insufficient to cover the proposed sharing activity, the data custodian or researcher must rely on another legal justification, for example, by seeking reconsent or a waiver of the requirement for consent. If an individual refused consent for the proposed sharing activity, no such sharing should take place.

An HREC or another ERB may authorise a waiver of the requirement to seek consent for sharing clinical trial data based on criteria specified in the National Statement and (if relevant) federal, state and territory privacy laws.
For an ERB to grant a waiver of the requirement for consent, the research must be lower risk, defined in the National Statement as:

Research in which there is no risk of harm, but in which there is a risk of discomfort and in which there may also be a foreseeable burden (low risk research) OR research in which there is no risk of harm or discomfort, but which includes a potential for minor burden or inconvenience (minimal risk research) (National Statement on Ethical Conduct in Human Research, 2023, p. 110).

In addition,

- the benefits of the research must outweigh the risk of harm from not seeking consent.
- It must be impracticable to obtain consent. Although the National Statement does not define impracticability, it does explain that it might apply 'due to the quantity, age or accessibility of records' (National Statement on Ethical Conduct in Human Research, 2023, para. 2.3.10(c)). Impracticability may arise where obtaining reconsent would place undue hardship on researchers, would invalidate study outcomes, or would harm participants or others, for example, by violating their privacy interests. (Laurijssen, 2022)
- There must be no reason to think the research participants would not have consented to the use or disclosure of their data.
- The privacy of participants must be sufficiently protected.
- The researcher or sponsor must have a plan to protect the confidentiality of data.
- There must be a plan to make results available to participants to protect their welfare to the extent practicable.
- The participants will not be deprived of financial benefits.
- The waiver must not be prohibited by State, federal or international law (National Statement on Ethical Conduct in Human Research, 2023, para. 2.3.10). For example, data disclosed by a patient to their general practitioner may be protected by the equitable duty of confidence. In these cases, a waiver of the requirement for consent may still not remove the requirement from patients to use their data (Adams et al., 2025, p. 853).

In deliberating on these criteria, ethics review bodies should be attuned to the participant group from which data has been obtained and the implications this may have for the ethical acceptability of a waiver of the requirement to seek consent. For example, in accordance with the principles of Indigenous Data Sovereignty, specialist Indigenous ethics review committees should be responsible for decision-making for the sharing of Indigenous data.

If the information satisfies the definition of personal information, additional requirements will apply before a waiver of the requirement for consent for sharing clinical trial data can be authorised. Under the National Statement, only an HREC (as compared with another ERB) may grant a waiver of consent for research

using personal information in medical research, or personal health information. The waiver may also need to satisfy the criteria set out in the Guidelines Approved under Sections 95 and 95A of the *Privacy Act 1988*. The Guidelines Approved under Section 95 of the *Privacy Act 1988* apply to personal information held by Commonwealth agencies for the purpose of medical research. The Guidelines Approved under Section 95A of the *Privacy Act 1988* apply to personal health information held by organisations for the purposes of research, or the compilation or analysis of statistics, relevant to public health or public safety. Both Guidelines require that an HREC make an assessment that the public interest in data sharing substantially outweighs the public interest in maintaining privacy protections. The Guidelines specify the information that a researcher must provide to the HREC to allow such an assessment, as well as the factors that should feed into an HREC's public interest assessment.

Some Australian states and territories also specify waiver of the requirement for consent requirements in their privacy laws, typically reliant on a specified public interest test and that obtaining consent would be 'impracticable'. **Appendix 2, Table 5** contains a breakdown of these requirements. In addition, in some cases, a particular government department might require its own ERB to authorise the use or disclose data held by a state or territory data custodian. For example, the Victorian Department of Justice and Community Safety has an internal research ethics committee (Wright et al., 2019, para. 2.64). Other data custodians may require approval by a HREC acting in accordance with the National Statement to release data (Coombs, 2019; Dickie, 2004, p. 14).

A final point to note is that Federal, state and territory privacy laws permit government agencies and private organisations to collect data without consent in certain circumstances. These circumstances include for public health, serious threats or life to health or where mandated under another law (*Privacy Act 1988* (Cth), s 16A(1), sch 1 cls 6.2(b); *Information Privacy Act 2014* (ACT), s 19(1)(a); *Health Records (Privacy and Access) Act 1997* (ACT), sch 1 cls 9.1(b)-(c), cls 10.2(d)-(e); *Privacy and Personal Information Protection Act 1998* (NSW), s 17(c), s 18(1)(c), s 19(2)(h); *Health Records and Information Privacy Act 2002* (NSW), sch 1 cls 10(1)(b1)-(c), cls 10(1)(b1)-(c); *Information Act 2002* (NT), sch 2 cls 2.1(d), cls 2.1(f); *Personal Information Protection Act 2004* (TAS), sch 1 cls 2(1)(d), 2(1)(f)-(g); *Privacy and Data Protection Act 2014* (VIC), sch 1 cls 2.1(d), 2.1(f)-(g); *Health Records Act 2001* (VIC), sch 1 cls 2.2(c), 2.2(h)). Public health laws also provide extensive powers for state and territory health departments to collect, use and disclose personal information without consent (*Public Health Act 1997* (ACT), s 109; *Public Health Act 2010* (NSW), s 98(6); *Public and Environmental Health Act 2011* (NT), ss 63-65; *Public Health Act 2005* (QLD), ch 3 part 1 div 3, ch 3 part 3 div 3, ch 6 part 1 div 4, ch 6 part 1A div 4, ch 6 part 2 div 4; *Public Health Act 2011* (SA), s 99(2)(a)-(c), s 99(2)(g)-(h), s 100(4)(c); *Public Health and Wellbeing Act 2008* (VIC), ss 55-7; *Public Health Act 2016* (WA), s 299). It is important to follow any procedures these laws set out for the use of personal information. Further, the Federal *Biosecurity Act* allows the Commonwealth Department of Health to share information in responding to public health risks (*Biosecurity Act 2015* (Cth), ss 582-585).

These laws authorise data sharing outside the scope of the human research ethics framework with which researchers and clinical triallists would otherwise need to comply. Further, data collected under these laws may be subsequently used for secondary purposes. However, even if there is a legal avenue to use this data under privacy, mental health or public health laws, there may be other legal or ethical barriers to secondary use. Using this data without appropriate consent or consulting with individuals whose information is included in a dataset could substantially disrupt public trust and social licence for that secondary use (Richards and Scheibner, 2022, p. 398). Therefore, personal information collected under these laws should not be assumed to be available for unrestricted secondary use. Wherever possible, individuals whose data has been obtained under these laws should be given control over its subsequent use and sharing. This is particularly important when considering data relating to Indigenous persons.

4. Optimise Collection Practices

It is imperative to anticipate the possibility of data sharing when designing the collection protocol for a research project or clinical trial (Pellen et al., 2023, pp. 2-3). Where possible, data custodians or researchers should collect personal information from participants directly, including through clear informed consent practices. However, it may not always be possible to collect data from participants, or doing so may result in additional burden to the participant (e.g. recollecting information that the participant has provided to another party). In these circumstances, data custodians and researchers should be cognisant of the additional safeguards that must be satisfied before sourcing data for secondary use.

a) Collecting information from primary care and administrative datasets

Primary care datasets can include electronic medical records and electronic health records. These records are compiled by health practitioners such as doctors at various times and in various locations. Under Australian law, health practitioners or their employers own the health records that they have compiled about a patient. Health practitioners also owe a duty of confidentiality to their patients (Adams et al., 2022b, p. 140). Therefore, health practitioners, hospitals and general practices should be treated as the data custodians of these records. These data custodians must seek explicit consent from their patients to enrol their records into research, clinical trials or quality improvement (Rowlands et al., 2024, p. 28).

In addition, administrative data may be collected or generated under statutory frameworks or by government agencies. These include datasets such as Medicare Benefit Schedule (MBS) or Pharmaceutical Benefit Scheme (PBS) data, as well as My Health Record. These administrative datasets also include datasets collected or generated by state or territory government agencies, such

as birth and death registries (Fahridin et al., 2024, p. 522). In these cases, legislation or other guidelines may state who is responsible for collecting information from primary care datasets (Framework to Guide the Secondary Use of My Health Record System Data, 2018, p. 31).

b) Data linkage

Data linkage is a method of bringing together information derived from different sources but relating to the same individual or event in a single file (Hobbs and McCall., 1970, p. 375). Data attributes such as names, dates of birth, addresses, sex and medical record numbers can be used to link datasets together (Research Governance Procedures, 2021, p. 31). For example, many clinical trial investigators and secondary researchers seek permission to access administrative datasets. These administrative datasets are then subsequently linked with clinical trial datasets for a variety of purposes, including tracking disease outcomes, survival status and health service usage (Fahridin et al., 2024, p. 522).

Linking two or more datasets—such as clinical trial data with administrative health records—can increase the risk of re-identifying individuals or individual records (National Health Information Standards and Statistics Committee, 2017, pp. 17–18). To minimise these privacy risks, additional safeguards are recommended. This includes engaging specialist data linkage units with expertise in secure linkage methodologies and access to high-security infrastructure. It is also generally recommended that the analyst working with the linked dataset does not have access to direct identifiers such as name, address, or date of birth. These practices help ensure that privacy is protected while enabling valuable secondary use of research data.

In addition, it may be necessary to seek consent from individuals in that administrative dataset, or a waiver of the requirement for consent from an ERB, to share their data (Fahridin et al., 2024, p. 522).

c) Other sources of clinical trial data, including publicly available information

Researchers or sponsors might have access to clinical trial data or datasets via other means, including via publicly available information. This information could include identifiable information or participant-level data. For publicly available datasets, the researcher or sponsor should see whether there is a data custodian who is available to contact. The data custodian may then help determine what privacy issues could arise from the use of the dataset. Depending on the contents of the dataset, a researcher or sponsor will need to comply with relevant privacy laws and seek ethics approval (National Statement on Ethical Conduct in Human Research, 2023, para. 3.1.51).

5. Establish Data Management Plans

Data security obligations include protecting personal data against theft, loss and unauthorised access, use, disclosure, copying or modification through technical and organisational processes. Trials should have clear data management plans for the systems and processes they will use to manage data retention, disposal, and access.

a) Data retention and disposal

The data custodian must ensure the researcher or sponsor has a plan for retaining or disposing of the data (Research Governance Procedures, 2021, p. 30).

By default, research data should be stored for at least 5 years (Management of Data and Information in Research: A Guide Supporting the Australian Responsible Conduct of Research, 2019, p. 3). However, if this data is used for clinical trials, it needs to be retained for at least 15 years and longer if participants were minors (commonly for 15 years after the minor reaches the age of 18). Clinical trial sponsors should also be mindful of product liability issues. Therefore, clinical trial records may need to be retained for longer than this 15-year period, (ICH Guideline for Good Clinical Practice, 2022, Section 5.5.11). Researchers should note the inherent tension between lengthy data retention practices and the data minimisation principle that specifies the need to destroy or deidentify information once it is no longer required for the purpose for which it was collected. In practice, this means that researchers should keep data securely and confidentially and should not keep multiple copies of the dataset.

Beyond these data storage requirements, if a data custodian, researcher or sponsor uses records from a Commonwealth authority, it will need to comply with the Commonwealth Archives Act. Likewise, if a data custodian, researcher or sponsor is a state or territory government agency, it will need to comply with applicable state or territory archive laws and regulations. **Appendix 2, Table 4** contains a breakdown of the disposal requirements under state and territory regulations.

b) Data access

A data custodian, data access committee or data custodian must ensure that those accessing the data comply with applicable privacy laws (Framework to Guide the Secondary Use of My Health Record System Data, 2018, p. 51). If there is a data breach, the data custodian should report any notifiable breaches to the appropriate regulatory agency. This agency could include the Office of the Australian Information Commissioner or an appropriate state and territory office. In the alternative, the data sharing agreement should specify who should report to the responsible regulatory agency.

Technology systems may be implemented to support secure access to data. One such technology-based approach is the requirement that data be accessed via a trusted research environment ('TRE') – also known as a secure research environment. A TRE is a remote access computing environment that allows an individual with appropriate credentials to access sensitive data for analytics purposes. The technological and governance controls applied to TREs mitigates the risk of sensitive data being accessed by unauthorised people or being used inappropriately (Rowlands et al., 2024, p. 27; Oppermann, 2017, p. 74). In some cases, the use of a TRE may be a precondition to accessing personal information held by a government agency. Under the *Data Availability and Transparency Act*, a Federal agency listed as an accredited data service provider can share data with designated parties via 'ADSP-controlled access'. This access involves the use of controls to prevent or minimise the risk that individuals may be re-identified from a dataset (*Data Availability and Transparency Act 2022* (Cth), s 16B(6)).

6. Assess Risks Before Sharing

The preceding principles and responsibilities address issues that should ideally be addressed at the initiation of a clinical trial to determine the intended approach for managing the sharing of data and documented in the approved protocol. To supplement these principles, data custodians should have a defined approach for assessing data sharing requests at the point they are received.

a) Risk Assessment

Before data sharing occurs (irrespective of whether consent has been sought), the data custodian, data access committee or data steward should assess the risk associated with sharing.

A common way of delineating these risks is the 'Five Safes' framework, which is a principles-based framework that provides a way to focus attention on the outcomes and objectives of data sharing. This approach has been recommended by the United States National Institute of Standards and Technology (NIST) for making government datasets available (Garfinkel et al., 2023, p. 34). In addition, some statutes mandate the use of the Five Safes framework as a means for assessing risk. For example, all ADSPs under the *Data Availability and Transparency Act* must ensure that the risk of any project is assessed with the Five Safes framework before sharing data (*Data Availability and Transparency Act 2022* (Cth), s 13(1)(e)). This model distinguishes between five key issues, each of which warrant attention—both independently and jointly—as part of a data sharing decision. (Desai et al., 2016, p. 4; Framework to Guide the Secondary Use of My Health Record System Data, 2018, p. 53). These issues are as follows:

1. **Safe Projects**, or the quality, integrity and transparency of the secondary research. Assessments of safe projects will resemble many frameworks for research ethics. (Oppermann, 2017, p. 70). Projects involving vulnerable populations, sensitive topics or participants from whom informed consent has not been sought could be assessed as having a moderate or low level of safety (Oppermann, 2017, pp. 69–71). See Section 3 for related discussion.

2. **Safe People**, or whether the secondary researcher's intention and character is such that they should be trusted to access and use the data appropriately. This process could involve checking the references and any conflicts of interest of the researcher or sponsor (Oppermann, 2017, p. 69). It may also require compliance with any ethics approval processes (Data Availability and Transparency Code 2022 (Cth), r 7).
3. **Safe Data**, or the disclosure risks inherent in the data being shared. This dimension requires an assessment of whether the granularity of disclosure for which sharing is sought is appropriate given the level of safety of the project and people. Depending on the results of this assessment, privacy preserving techniques may be applied and/or governance strategies ('Safe Settings') adopted. (Oppermann, 2017, pp. 76–80). See Section 2 for related discussion.
4. **Safe Settings**, or the access controls in place for a secondary researcher. Systems with no access restrictions in place are at one end of the Safe Settings risk continuum through to, for example, systems with multi-factor authentication, audit trails, and preventing on-sharing (Oppermann, 2017, p. 72). TREs are intended to provide safe settings but specific TREs may rate differently on the continuum. See Section 5(b) for related discussion.
5. **Safe Outputs**, or whether any published statistical results reveal the identity of individuals (Multi-Agency Data Integration Project (MADIP) Privacy Impact Assessment Update, 2019, p. 25). An evaluation of Safe Output requires a consideration of the value of the data being shared and a project's overall level of safety. (Oppermann, 2017, pp. 76–80).

In totality, the aim is to review for 'safe' data sharing conditions, but this does not require each of the dimensions to constitute 'maximum safety' (Ritchie, 2017, p. 2). The framework is highly dependent on judgment, and there is no unambiguous way of quantifying a threshold level of safety for sharing. Oppermann provides examples of strategies that can be used to minimise the risks associated with data sharing within the Five Safes framework (Oppermann, 2017, p. 71, 76). Rodriguez and others also utilise a framework developed by Dankar and others to assess the identifiability risk associated with different clinical trials dataset (Dankar et al., 2012, p. 2-8; Rodriguez et al., 2025, p. 2). Likewise, a data custodian, data access committee or data steward could use a similar approach to assess the 'safe data' dimension of five safes and therefore reduce the risk of disclosure using the other four dimensions.

b) Special Considerations

(i) On-sharing administrative data collections

Administrative data collections are typically held by a federal, state or territory government department or public agency and may require specific authorisations for sharing. In some cases, Commonwealth datasets such as MBS and PBS data will be held by Commonwealth departments, or Commonwealth agencies. For example, the Australian Institute of Health and Welfare (AIHW) is the responsible data custodian for My Health Record data (Framework to Guide the Secondary Use of My Health Record System Data, 2018, pp. 4, 8).

Access to this data for secondary research will require a request to the responsible data custodian. To link two or more datasets together, approval is required from all data custodians. This linkage should be conducted by a trusted third party.

In addition, the data custodian for the administrative dataset may not have consent from individuals in that dataset to use their data for secondary purposes. Accordingly, it may be necessary for the investigator to either seek consent from participants or seek a waiver of the requirement for consent from an ERB (Fahridin et al., 2024, p. 522).

(ii) Adding clinical trial datasets to data repositories

Data repositories are a research infrastructure service that enable researchers to delegate parts or all their data governance, storage and management, and/or access responsibilities to a third-party provider (Xafis & Labude, 2019). Data repositories create a centralised pool of data from multiple trials designed to be discoverable for researchers to access and reuse (Xafis & Labude, 2019, pp. 256-257). Some but not all data repositories host individual participant-level data (Banzi et al., 2019, p. 6). In addition to providing secondary researchers a single platform to discover data from multiple trials, repositories often providing a mechanism to request access to data, and may also provide secure platforms for accessing and working on data. Repositories vary greatly in terms of which of these features they offer and the level of delegation that data custodians can assign to the repository. For example, in the USA, the Vivli service stores participant data, reviews data sharing requests, and provides a data access platform on behalf of the clinical trials using their service (Banzi et al., 2019, pp. 6-7). In contrast, the Health Data Australia platform does not store data or provide a data access platform. Instead, it consists of a catalogue of data held by Australian data custodians and allows secondary researchers to submit a data sharing request which is sent to the respective custodian to review and respond in accordance with their individual governance requirements. As such, it assists trials who wish to share data but would not be classified as a data repository (Health Data Australia, 2023).

Although not binding in Australia, the European Federation of Pharmaceutical Industries and Associations and the Pharmaceutical Research and Manufacturers of America (PhRMA) have published their own guides on data sharing. These guidelines require pharmaceutical companies to share participant level data from registered clinical trials with qualified researchers, which may include adding data to a repository (Principles for Clinical Trial Data Sharing, 2023, p. 1). Some clinical trial funders and medical journal editors require data management plans, including how the data underpinning clinical trial results will be shared through approaches such as data repositories (Banzi et al., 2019, p. 6).

Clinical trial datasets containing participant-level data should only be added to data repositories with the consent of participants. Data should be de-identified before being added (Principles for Clinical Trial Data Sharing, 2023, p. 2). Consent to add clinical trial data to data repositories should be sought from

participants when they are enrolled in the original trial (Wizemann et al., 2020, pp. 17–18). De-identification could involve aggregating potentially identifiable data such as survival or adverse event data. Alternatively, participant-level data could be made accessible to researchers via a trusted research environment from which data cannot be downloaded (Modi et al., 2023, pp. 403–405).

(iii) Sending data overseas or to foreign or dual nationals
Any sharing of clinical trial data with a non-Australian researcher or sponsor must comply with Australian law. Depending on which data custodian holds the data, these could include Commonwealth, state or territory laws, or a combination of all three. A data custodian may also have other criteria that they may wish to place on use of or disclosure to a non-Australian researcher or sponsor. These include partnership with an Australian entity, proposed public health benefits to Australians or a requirement that data remain in Australia (Framework to Guide the Secondary Use of My Health Record System Data, 2018, p. 23). In addition, any data which is shared with Australian researchers by overseas researchers may be covered by overseas data privacy laws. These laws include the General Data Protection Regulation (GDPR) from the European Union and the Health Insurance Portability and Accountability Act (HIPAA) from the United States. When data is transferred from an overseas jurisdiction subject to these or other laws, the researcher or sponsor in Australia should ensure that any handling of this data is compliant both with these laws and the applicable law in Australia.

7. Engage with Participant Groups

Those developing clinical research data sharing frameworks should consult with relevant consumer groups to incorporate lived experience perspectives. Although each consumer group will have specific considerations relevant to data sharing frameworks, particular attention is warranted for Aboriginal and Torres Strait Islander communities and rare disease patients.

a) Indigenous research participants

Historically, Indigenous communities have not had appropriate control over the way their data has been used. In particular, the use of Indigenous data has often failed to comply with the wishes of Indigenous participants and health consumers and has exposed individuals and their communities to risk. Accordingly, the Indigenous Data Sovereignty movement has sought for Indigenous peoples to have greater control over the data about Indigenous peoples (both as individuals and communities) and Indigenous knowledge (Carroll et al., 2021).

Through Indigenous Data Sovereignty, Aboriginal and Torres Strait Islander peoples and communities are seeking to regain sovereignty and governance over data that relates to them. The objectives of Indigenous Data Sovereignty are consistent with Article 31 of the United Nations Declaration on the Rights of Indigenous People (UNDRIP), which states that Indigenous people have a right to control their cultural heritage.

The CARE Principles for Indigenous Data Governance provide a framework for operationalising Article 31 and addressing Indigenous concerns regarding the use of data (CARE Principles, 2018; Caroll et al., 2021). These principles are elaborated in more detail below:

1. **Collective benefit:** Data must be collected, used and shared so that Indigenous peoples can derive benefit from that data. This benefit can include improved governance as well as policy development and service delivery.

2. **Authority to Control:** Indigenous people have rights over both their knowledge and data, and therefore this knowledge and data can only be used with free, informed and prior consent. Indigenous knowledge and data should be used to enable Indigenous self-determination.

3. **Responsibility:** Researchers and policy makers who work with Indigenous data have a duty to explain how that data can benefit Indigenous peoples and enable self-determination.

4. **Ethics:** The rights and wellbeing of Indigenous peoples and communities should be central to any ethical processes regarding the use of data. These ethical processes should also recognise any imbalances in power and resources.

Following the CARE Principles, Aboriginal and Torres Strait Islander peoples have a right to exercise control over the creation, development, stewardship, and analysis of their information. This is reflected in the Australian Institute of Aboriginal and Torres Strait Islander Studies (AIATSIS) Code of Ethics for Aboriginal and Torres Strait Islander Research. This Code of Ethics advises that processes should be agreed at an early stage for ownership, management and use of, access to, and distribution of research results relating to Indigenous knowledge and data (Australian Institute of Aboriginal and Torres Strait Islander Studies (AIATSIS), 2022, para. 2.7(b)).

Data custodians, researchers and sponsors conducting research relating to Aboriginal and Torres Strait Islander communities should partner with these communities in developing data sharing frameworks. This could be achieved by including Aboriginal and Torres Strait Islander people in existing data access committees or developing new Aboriginal and Torres Strait Islander governance committees (Framework for Governance of Indigenous Data, 2024, p. 13-14). Data custodians should also develop resources to help develop understanding of Indigenous Data Sovereignty, identify datasets that contain Indigenous data and develop specific data access policies (Framework for Governance of Indigenous Data, 2024, p. 15-19).

Data custodians, researchers and sponsors should ensure they collect personal information from Aboriginal and Torres Strait Islander persons according to the Free Prior and Informed Consent Principles (FPIC). Under FPIC, individuals and communities should have the right to withdraw or modify their consent at any time (Schroeder, 2009, pp. 47-8). Accordingly, forms of consent such as bundled and unspecified consent generally should not be used for research involving Aboriginal and Torres Islander people or communities. Instead, individuals should have clear mechanisms to modify or withdraw their consent (Teare et al, 2021, pp. 651-2).

These mechanisms may override the existing principles associated with access to or erasure of clinical trial data discussed in Section 3.

In Aboriginal and Torres Strait Islander communities, there also is a concept of 'community privacy'. Even where a dataset does not contain identifiable data, it may be possible to identify an Aboriginal or Torres Strait Islander community. Any data which could be used to identify a specific community should not be released without that community's consent (NT Health Data Release Guidelines, 2018, p. 7). All research involving data collected from Aboriginal or Torres Strait Islander communities must be approved by an ERB with expertise in Aboriginal research.

b) Rare disease patients

Due to small cell sizes, it may be possible to identify patients with rare diseases, even if steps have been taken to de-identify that data. Therefore, data custodians, data access committees and data custodians should determine whether individuals can be identified from such datasets. This risk should be assessed when considering the safe data rating as discussed in Section 6. Depending on the size of the cohort of individuals with the rare disease, in some cases it may be impossible to fully guarantee anonymity, particularly for open data sets (Rubinstein et al., 2020, p. 475). In this situation, the data custodian, researcher or sponsor must ensure that appropriate informed consent is obtained for the use of this data.

References:

Adams, C., Flack, F., & Allen, J. (Eds.). (2022a). Better Practice and Processes. In *Sharing Linked Data for Health Research: Toward Better Decision Making* (pp. 206–240). Cambridge University Press. https://doi.org/10.1017/9781108675789.010

Adams, C., Flack, F., & Allen, J. (Eds.). (2022b). Law. In *Sharing Linked Data for Health Research: Toward Better Decision Making* (pp. 131–174). Cambridge University Press. https://doi.org/10.1017/9781108675789.008

Adams, C., Flack, F., & Allen, J. (Eds.). (2022c). Research Using Linked Data. In *Sharing Linked Data for Health Research: Toward Better Decision Making* (pp. 11–27). Cambridge University Press. https://doi.org/10.1017/9781108675789.003

Adams, C., Braunack-Mayer, A., & Flack, F. (2025). Access to general practice data for research in Australia: The need for greater clarity in relation to privacy and confidentiality. *Journal of Law and Medicine*, *31*(4), 840–855. https://doi.org/10.3316/informit.T202503290000779068116261O

Australian Institute of Aboriginal and Torres Strait Islander Studies (AIATSIS). (2022). *AIATSIS Code of Ethics for Aboriginal and Torres Strait Islander Research*. Code of Ethics for Aboriginal and Torres Strait Islander Research.

Banzi, R., Canham, S., Kuchinke, W., Krleza-Jeric, K., Demotes-Mainard, J., & Ohmann, C. (2019). Evaluation of repositories for sharing individual-participant data from clinical studies. *Trials*, *20*(1), 169. https://doi.org/10.1186/s13063-019-3253-3

CARE Principles. (2018, November 8). Global Indigenous Data Alliance. https://www.gida-global.org/care

Carroll, S. R., Herczog, E., Hudson, M., Russell, K., & Stall, S. (2021). Operationalizing the CARE and FAIR Principles for Indigenous data futures. *Scientific Data*, *8*(1), 108. https://doi.org/10.1038/s41597-021-00892-0

Coombs, E. (2019). *Statutory Guidelines on Research—Section 27B* [Information and Privacy Commission New South Wales]. https://www.ipc.nsw.gov.au/sites/default/files/2020-01/Statutory_Guidelines_on_Research_section_27B_September_2019.pdf

Dankar, F. K., El Emam, K., Neisa, A., & Roffey, T. (2012). Estimating the re-identification risk of clinical data sets. *BMC Medical Informatics and Decision Making*, *12*(1), 66. https://doi.org/10.1186/1472-6947-12-66

Data Access and Release Policy. (2023). Independent Health and Aged Care Pricing Authority. https://www.ihacpa.gov.au/sites/default/files/2023-09/data_access_and_release_policy_v7.0_-_review_2023.pdf

Data Retention When Subjects Withdraw from FDA-Regulated Clinical Trials (Guidance Document FDA-2008-D-0576). (2008). FDA. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/data-retention-when-subjects-withdraw-fda-regulated-clinical-trials

Desai, T., Ritchie, F., & Welpton, R. (2016). *Five Safes: Designing data access for research* (20161601; Working Papers). Department of Accounting Economics and Finance, Bristol Business School, University of the West of England. https://ideas.repec.org//p/uwe/wpaper/20161601.html

Dickie, J. (2004). *Statutory Guidelines on Research:* Health Records and Information Privacy Act 2002 *(NSW)* [Information and Privacy Commission New South Wales]. https://www.ipc.nsw.gov.au/sites/default/files/file_manager/privacy_statutory_guidelines_research.pdf

Eckstein, L., Garrett, J. R., & Berkman, B. E. (2014). A framework for analyzing the ethics of disclosing genetic research findings. *The Journal of Law, Medicine & Ethics: A Journal of the American Society of Law, Medicine & Ethics*, *42*(2), 190–207. https://doi.org/10.1111/jlme.12135

Eckstein, L., Otlowski, M., Taylor, M., & McWhirter, R. (2023). Reversing the “Quasi-Tribunal” Role of Human Research Ethics Committees: A Waiver of Consent Case Study Thematic: Life Sciences: Ethics, Innovation and the Future of Law. *University of New South Wales Law Journal*, *46*(2), 498–534.

Fact Sheet—Consent. (2023, June). Information and Privacy Commission NSW. https://www.ipc.nsw.gov.au/fact-sheet-consent, https://www.ipc.nsw.gov.au/fact-sheet-consent

Fahridin, Salma, Neeru Agarwal, Karen Bracken, Stephen Law, and Rachael L. Morton. 2024. “The Use of Linked Administrative Data in Australian Randomised Controlled Trials: A Scoping Review.” *Clinical Trials* 21(4):516–25. doi:10.1177/17407745231225618.

Framework for Governance of Indigenous Data (2024). Australian Bureau of Statistics. Available at: https://www.niaa.gov.au/sites/default/files/documents/2024-05/framework-governance-indigenous-data.pdf.

Framework to Guide the Secondary Use of My Health Record System Data. (2018). Department of Health and Aged Care. https://www.health.gov.au/sites/default/files/documents/2021/12/framework-to-guide-the-secondary-use-of-my-health-record-system-data.pdf

Garfinkel, S., Guttman, B., Near, J., Dajani, A., & Singer, P. (2023). *De-Identifying Government Datasets: Techniques and Governance* (NIST Special Publication (SP) 800-188). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-188

Green, E., & Ritchie, F. (2023). The present and future of the Five Safes framework. *Journal of Privacy and Confidentiality*, *13*(2), Article 2. https://doi.org/10.29012/jpc.831

Guidelines Under Section 95 of the Privacy Act 1988. (2024). National Health and Medical Research Council. https://www.nhmrc.gov.au/about-us/publications/guidelines-under-section-95-privacy-act-1988

Guide—Privacy and persons with reduced decision-making capacity. (2021, November). Information and Privacy Commission NSW. https://www.ipc.nsw.gov.au/guide-privacy-and-persons-reduced-decision-making-capacity, https://www.ipc.nsw.gov.au/guide-privacy-and-persons-reduced-decision-making-capacity

Haas, M. A., Madelli, E. O., Brown, R., Prictor, M., & Boughtwood, T. (2024). Evaluation of CTRL: A web application for dynamic consent and engagement with individuals involved in a cardiovascular genetic disorders cohort. *European Journal of Human Genetics*, *32*(1), 61–68. https://doi.org/10.1038/s41431-023-01454-1

Health Data Australia. (2023, July). Australian Research Data Commons. https://researchdata.edu.au/health/

Hobbs, M. S. T., and M. G. McCall. 1970. “Health Statistics and Record Linkage in Australia.” *Journal of Chronic Diseases* 23(5): 375–81. doi:10.1016/0021-9681(70)90020-2.

Hocking, L., Parks, S., Altenhofer, M., & Gunashekar, S. (2019). *Reuse of health data by the European pharmaceutical industry: Current practice and implications for the future*. RAND Corporation. https://www.rand.org/pubs/research_reports/RR3247.html

Hunter, K. *et al.* (2024) *Secondary use of clinical trials data in health research: A Practical Guide*. Australian Research Data Commons. Available at: https://doi.org/10.5281/zenodo.12768050.

ICH Guideline for Good Clinical Practice. (2022). Therapeutic Goods Administration (TGA). https://www.tga.gov.au/resources/publication/publications/ich-guideline-good-clinical-practice

Kind, C. (2025, July 31). *Report into preliminary inquiries of I-MED*. OAIC. https://www.oaic.gov.au/privacy/privacy-assessments-and-decisions/privacy-decisions/Investigation-inquiry-reports/report-into-preliminary-inquiries-of-i-med

Krebs, S. and Moses, L.B. (2024) 'Data Sharing Agreements: Contracts for Access to Personal Information in the Digital Age', *Melbourne University Law Review*, 48(1), pp. 95–151.

Lalova-Spinks, T., De Sutter, E., Valcke, P., Kindt, E., Lejeune, S., Negrouk, A., Verhenneman, G., Derèze, J.-J., Storme, R., Borry, P., Meszaros, J., & Huys, I. (2022). Challenges related to data protection in clinical research before and during the COVID-19 pandemic: An exploratory study. *Frontiers in Medicine*, *9*. https://doi.org/10.3389/fmed.2022.995689

Laurijssen, Sara JM, et al. "When is it impractical to ask informed consent? A systematic review." *Clinical Trials* 19.5 (2022): 545-560.

Management of data and information in research: A guide supporting the Australian Responsible Conduct of Research. (2019). National Health and Medical Research Council. https://www.nhmrc.gov.au/file/14359/download?token=L5GTBw96

Modi, N. D., Kichenadasse, G., Hoffmann, T. C., Haseloff, M., Logan, J. M., Veroniki, A. A., Venchiarutti, R. L., Smit, A. K., Tuffaha, H., Jayasekara, H., Manning-Bennet, A., Morton, E., McKinnon, R. A., Rowland, A., Sorich, M. J., & Hopkins, A. M. (2023). A 10-year update to the principles for clinical trial data sharing by pharmaceutical companies: Perspectives based on a decade of literature and policies. *BMC Medicine*, *21*(1), 400. https://doi.org/10.1186/s12916-023-03113-0

Moses, L. B. (2020). Who owns information?: Law enforcement information sharing as a case study in conceptual confusion. *University of New South Wales Law Journal*, *43*(2), 615–641. https://doi.org/10.3316/informit.238185290220023

Morten, C. J., Nicholas, G., & Viljoen, S. (2024). Researcher Access to Social Media Data: Lessons from Clinical Trial Data Sharing. *Berkeley Technology Law Journal*, *39*(1), 109–204.

Multi-Agency Data Integration Project (MADIP) Privacy Impact Assessment Update. (2019). Australian Bureau of Statistics. https://www.abs.gov.au/about/legislation-and-policy/privacy/privacy-impact-assessments/2019%20MADIP%20PIA%20Update%20-%20PIA%20Report.pdf

National Clinical Trials Governance Framework Literature Review. (2018). Australian Commission on Safety and Quality in Health Care. https://www.safetyandquality.gov.au/publications-and-resources/resource-library/national-clinical-trials-governance-framework-literature-review

National Health Information Standards and Statistics Committee. (2017). *Guidelines for the Disclosure of Secondary Use Health Information for Statistical Reporting, Research and Analysis*. Australian Institute of Health and Welfare. https://www.aihw.gov.au/getmedia/d15f8bf7-f29f-406a-a27d-41f483b17ff1/Guidelines-Use-and-disclosure-of-secondary-health-information-endorsed-15-June-2017.pdf.aspx

National Statement on Ethical Conduct in Human Research. (2023). National Health and Medical Research Council. https://www.nhmrc.gov.au/about-us/publications/national-statement-ethical-conduct-human-research-2023

NT Health data release guidelines. (2018). Northern Territory Government | Department of Health. https://hdl.handle.net/10137/7106

Oppermann, I. (2017). *Data Sharing Frameworks—Technical Whitepaper*. Australian Computer Society. https://www.acs.org.au/content/dam/acs/acs-publications/ACS_Data-Sharing-Frameworks_FINAL_FA_SINGLE_LR.pdf

Otlowski, M. F. A. (2012). Tackling legal challenges posed by population biobanks: Reconceptualising consent requirements. *Medical Law Review*, *20*(2), 191–226. https://doi.org/10.1093/medlaw/fwr035

Pellen, C., Louarn, A. L., Spurrier-Bernard, G., Decullier, E., Chrétien, J.-M., Rosenthal, E., Goff, G. L., Moher, D., Ioannidis, J. P. A., & Naudet, F. (2023). Ten (not so) simple rules for clinical trial data-sharing. *PLOS Computational Biology*, *19*(3), e1010879. https://doi.org/10.1371/journal.pcbi.1010879

Privacy Act Review Report. (2023). Attorney-General's Department. *https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report*

Principles for accessing and using publicly funded data for health research. (2016). National Health and Medical Research Council. https://www.nhmrc.gov.au/sites/default/files/documents/reports/principles-publically-funded-data.pdf

Principles for Clinical Trial Data Sharing. (2023). European Federation of Pharmaceutical Industries and Associations (EFPIA), Pharmaceutical Research and Manufacturers of America. https://phrma.org/resource-center/Topics/Clinical-Trials/PhRMA-Principles-for-Clinical-Trial-Data-Sharing

Research Governance Procedures. (2021). Western Australian Department of Health. https://www.health.wa.gov.au/~/media/Corp/Policy-Frameworks/Research/Research-Governance-Policy/Supporting/Research-Governance-Procedure.pdf

Researcher User Guide. (2023). Queensland Health. https://www.health.qld.gov.au/__data/assets/pdf_file/0027/1247724/qld-health-researcher-user-guide.pdf

Richards, B., & Scheibner, J. (2022). Health technology and big data: Social licence, trust and the law. *Journal of Law and Medicine*, *29*(2), 388–399.

Ritchie, F. (2017). The 'Five Safes': A framework for planning, designing and evaluating data access solutions. *Data for Policy Conference*. https://uwe-repository.worktribe.com/index.php/preview/880718/99_Ritchie.pdf

Rodriguez, A., Williams, L. J., Lewis, S. C., Sinclair, P., Eldridge, S., Jackson, T., & Weir, C. J. (2025). Evaluating re-identification risks scores in publicly available clinical trial datasets: Insights and implications. *Clinical Trials*, 17407745251356423. https://doi.org/10.1177/17407745251356423

Rowlands, D., Steele, M., Fung, M., & Corell, P. (2024). *Data Governance Framework*. New South Wales Department of Health. https://www.health.nsw.gov.au:443/lumos/Pages/data-governance-framework.aspx

Rubinstein, Y.R. et al. (2020) 'The case for open science: rare diseases', *JAMIA Open*, 3(3), pp. 472–486. Available at: https://doi.org/10.1093/jamiaopen/ooaa030.

Schneider, M., Radbone, C., Vasquez, S., Palfy, M., & Stanley, A. (2019). Population Data Centre Profile: SA NT DataLink (South Australia and Northern Territory). *International Journal of Population Data Science*, *4*(2), 1136. https://doi.org/10.23889/ijpds.v4i2.1136

Tassé, A.-M. (2016). A Comparative Analysis of the Legal and Bioethical Frameworks Governing the Secondary Use of Data for Research Purposes. *Biopreservation and Biobanking*, *14*(3), 207–216. https://doi.org/10.1089/bio.2015.0121

Teare, H. J. A., Prictor, M., & Kaye, J. (2021). Reflections on dynamic consent in biomedical research: The story so far. *European Journal of Human Genetics*, *29*(4), 649–656. https://doi.org/10.1038/s41431-020-00771-z

Thorogood, A. and Knoppers, B.M. (2017) 'Can research ethics committees enable clinical trial data sharing?', *Ethics, Medicine and Public Health*, 3(1), pp. 56–63. Available at: https://doi.org/10.1016/j.jemep.2017.02.010.

Wilkinson, M. D., Dumontier, M., Aalbersberg, Ij. J., Appleton, G., Axton, M., Baak, A., Blomberg, N., Boiten, J.-W., da Silva Santos, L. B., Bourne, P. E., Bouwman, J., Brookes, A. J., Clark, T., Crosas, M., Dillo, I., Dumon, O., Edmunds, S., Evelo, C. T., Finkers, R., … Mons, B. (2016). The FAIR Guiding Principles for scientific data management and stewardship. *Scientific Data*, *3*(1), 160018. https://doi.org/10.1038/sdata.2016.18

Wizemann, T., Khandekar, E., Hinners, J., & Shore, C. (Eds.) (with Forum on Drug Discovery, Development, and Translation, Forum on Neuroscience and Nervous System Disorders, National Cancer Policy Forum, Roundtable on Genomics and Precision Health, Board on Health Sciences Policy, Board on Health Care Services, Health and Medicine Division, & National Academies of Sciences, Engineering, and Medicine). (2020). *Reflections on Sharing Clinical Trial Data: Challenges and a Way Forward: Proceedings of a Workshop*. National Academies Press. https://doi.org/10.17226/25838

Wright, F., Forte, J., May, S., Ford, C., Pollock, A., & Bendall, A. (2019, November 14). *IPP 2 – Use and Disclosure*. Office of the Victorian Information Commissioner. https://ovic.vic.gov.au/book/ipp-2-use-and-disclosure/

Xafis, V., & Labude, M. K. (2019). Openness in Big Data and Data Repositories. *Asian Bioethics Review*, *11*(3), 255–273. https://doi.org/10.1007/s41649-019-00097-z

Appendix 1: Methods

Legislative Review

This method involved a purposive search for all legislative instruments that govern the use, collection and disclosure of data for clinical trials. A similar legislative protocol was conducted by Tassé in 2016 of the legal and bioethical frameworks governing the secondary use of data for research purposes (Tassé, 2016, p. 208). This review focused on literature and legislation from Australia, Canada, France, the United Kingdom and the United States. It also included literature from PubMed and Google Scholar. Likewise, another similar protocol was developed by Eckstein, Garrett and Berkman to identify literature on the disclosure of genetic research findings to participants (Eckstein et al., 2014, pp. 192–193). Finally, a similar approach has been used by the Australian Commission on Safety and Quality in Health Care to conduct a review of clinical trials governance frameworks (National Clinical Trials Governance Framework Literature Review, 2018, pp. 4–5). These legislative instruments were separated into three categories. The first category includes legislation relevant to clinical data sharing and secondary use of data, including personal and health information. The second category includes regulation relevant to consent to medical treatment and research, including consent to involvement by a clinical research team. The third category included legislation, regulations and other instruments governing the storage of documents and data relevant to clinical trials.

Grey Literature Review of Data Sharing Frameworks

To identify relevant ethical frameworks in Australia, a purposive search for existing documents was conducted. These included frameworks for secondary data sharing published by Australian government agencies, as well as those published by regulatory bodies. A search was conducted using Google Advanced Search to identify all documents which referred to the terms ‘secondary use health data ethical principles’ on websites with the gov.au domain. Each document was then read and filtered to see whether it contained a set of ethical or operational principles with respect to data sharing. Documents that were more than 10 years old were removed to ensure that only guidelines referencing recent legislation remained. Likewise, other documents (such as protocols and data sharing templates) were excluded. In addition to these documents, a comprehensive but non-exhaustive list of secondary sources, including journal articles and book chapters, were included to supplement these findings.

Appendix 2: Legislation and Guidelines

Table 1: Australian legislation and regulations relevant to clinical data sharing and secondary use of clinical data (including personal and health information), divided by type and jurisdiction:

Jurisdiction	Privacy Legislation	Health Privacy Legislation	Other Health Legislation	Other Heath Regulations
Commonwealth	*Privacy Act 1988*	*Healthcare Identifiers Act 2010* *Healthcare Identifiers Regulations 2020* *My Health Records Act 2012*	*National Health Act 1953* *National Health (Privacy) Rules 2021* *Health Insurance Act 1973* *Australian Institute of Health and Welfare Act 1987* *Biosecurity Act 2015* *Australian Institute of Health and Welfare (Ethics Committee) Regulations 2018* *Therapeutic Goods Act 1989* *Therapeutic Goods Regulations 1990*	Guidelines approved under section 95 of the Privacy Act 1988 (NHMRC) Guidelines approved under section 95A of the Privacy Act Therapeutic Goods Administration, Note on ICH Guideline on Good Clinical Practice, 2018

				AIATSIS Code of Ethics for Aboriginal and Torres Strait Islander Research (2020)
Australian Capital Territory	*Information Privacy Act 2014*	*Health Records (Privacy and Access) Act 1997*	*Public Health Act 1997*	
New South Wales	*Privacy and Personal Information Protection Act 1998*	*Health Records and Information Privacy Act 2002* *Health Records and Information Privacy Regulation 2022* *Health Records and Information Privacy Code of Practice 2005* *Health Administration Regulation 2010*	*Mental Health Act 2007* *Public Health Act 2010* *Public Health Regulation 2022*	Information Privacy Commissioner, Statutory Guidelines on Research 2019 Information Privacy Commissioner, Statutory Guidelines on Research (Health Records and Information Privacy Act 2002) 2004 Hunter and New England Health, Guide to Completing the Human Research Ethics Application (HREA) in REGIS 2021
Northern Territory	*Information Act 2002*	N/A	*Medicines, Poisons and Therapeutic Goods Act 2012*	

			Mental Health and Related Services Act 1998 *Public and Environmental Health Act 2011* *Public and Environmental Health Regulations 2014*	
Queensland	*Information Privacy Act 2009*	N/A	*Hospital and Health Boards Act 2011* *Mental Health Act 2016* *Public Health Act 2005* *Public Health Regulation 2018*	Queensland Health, Research User Guide 2025 Queensland Health, Guideline – Disclosure of Confidential Information for Research 2023
South Australia	N/A	N/A	*Guardianship and Administration Act 1993* *Health Care Act 2008* *Public Health Act 2011* *Mental Health Act 2009* *Transplantation and Anatomy Act 1993*	SA Health, Research Ethics and Governance Policy 2025 SA Health, National Mutual Acceptance Single Ethical Review of Multi-centre Human Research Projects Standard Principles for Operation 2022

Tasmania	*Personal Information Protection Act 2004*	N/A	*Mental Health Act 2013* *Public Health Act 1997*	
Victoria	*Privacy and Data Protection Act 2014*	*Health Records Act 2001*	*Health Services Act 1988* *Mental Health and Wellbeing Act 2022* *Public Health and Wellbeing Act 2008*	
Western Australia	*Privacy and Responsible Information Sharing Bill 2024*	N/A	*Health Services Act 2016* *Health Services (Information) Regulations 2017* *Mental Health Act 2014* *Public Health Act 2016*	Department of Health, Research Governance Procedures 2021

Table 2: Australian legislation, regulations and policies relevant to consent to medical treatment and research (including clinical research), divided by type and jurisdiction

	Legislation Governing Consent	Consent Regulations	Policies and Guidelines Relevant to Consent
Australian Capital Territory	*Guardianship and Management of Property Act 1991* *Medical Treatment (Health Directions) Act 2006* *Mental Health Act 2015* *Powers of Attorney Act 2006* *Children and Young People Act 2008*	*Children and Young People (Research) Standards 2023*	
New South Wales	*Guardianship Act 1987*	*Guardianship Regulation 2016*	*Clinical Trials – Insurance and Indemnity 2011* *Human Research Ethics Committees: Standards for Scientific Review of Clinical Trials 2007* *Safety Monitoring and Reporting for Clinical Trials Conducted in NSW Public Health Organisations 2017* *Operations Manual: Human Research Ethics Committee Executive Officers 2010* *Operations Manual: Research Governance Officers 2010*

			Authorisation to Commence Human Research in NSW Public Health Organisations 2010 *Information and Privacy Commission, Fact Sheet on Consent 2023* *Information and Privacy Commissioner, Privacy and Persons with Reduced Decision Making Capacity 2021*
Northern Territory	*Guardianship of Adults Act 2016* *Advance Personal Planning Act 2013*		
Queensland	*Guardianship and Administration Act 2000* *Child Protection Act 1999*		*Queensland Health Research Management Policy 2022* *Standard Operating Procedures for Queensland Health Research Governance Officers 2025* *Standard Operating Procedures for Queensland Health Human Research Ethics Committee (HREC) Administrators 2024* *Queensland Health Researcher User Guide 2025*
South Australia	*Guardianship and Administration Act 1993* *Consent to Medical Treatment and Palliative Care Act 1995*		*Research Ethics and Governance Policy 2025*
Tasmania	*Guardianship and Administration Act 1995*		*University of Tasmania Clinical Trials Procedure 2025*

Victoria	*Medical Treatment Planning and Decisions Act 2016*		*Research Governance and Site Specific Assessment 2024* Additional advice published by the Victorian State Government
Western Australia	*Guardianship and Administration Act 1990*	*Guardianship and Administration Regulations 2005*	*Research Policy Framework 2025* *Research Governance Policy 2021* *Research Governance Procedures 2021*

Table 3: Australian legislation, regulations and policies relevant to storage, ownership and transfer of clinical data, divided by type and jurisdiction

	Data Storage Legislation	Other potentially relevant laws	Data Storage Regulations, Policies and Guidelines
Commonwealth	*Archives Act 1983* *Census and Statistics Act 1905*	*Data Availability and Transparency Act 2022* *Copyright Act 1968* *Freedom of Information Act 1982*	*Therapeutic Goods Administration, Note for Guidance on Good Clinical Practice* Australian Code for the Responsible Conduct of Research, Management of data and information in research
Australian Capital Territory	*Health Records (Privacy and Access) Act 1997* *Territory Records Act 2002*	*Births, Deaths and Marriages Registration Act 1997* *Freedom of Information Act 2016*	*Territory Records (Records Disposal Schedule – Health Treatment and Care Records) Approval 2023* *Territory Records (Records Disposal Schedule – Patient Services Administration Records) Approval 2013 (No 1)* *Territory Records (Records Disposal Schedule – Population Health Care Management and Control Records 2009 (No 1)*
New South Wales	*State Records Act 1998*	*Births, Deaths and Marriages Registration Act 1995*	*GDA-17-General Retention and Disposal Authority Public health services: patient/client records* *GDA-21-General Retention and Disposal Authority Public health services: administrative records*

		Data Sharing (Government Sector) Act 2015 *Government Information (Public Access) Act 2009*	
Northern Territory	*Information Act 2002*	*Births, Deaths and Marriages Registration Act 1996*	*Northern Territory Public Sector Organisations Records and Information Management Standard* *Functional Records Disposal Schedules, Department of Territory Families, Housing and Communities* *Records Disposal Schedule, Alcohol and Other Drugs Services, Department of Health (No. 2017/7)* *Records Disposal Schedule, Centre for Disease Control, Department of Health (No. 2014/22)* *Records Disposal Schedule, National Critical Care and Trauma Response, National Critical Care and Trauma Response Centre, Department of Health (No. 2015/10)* *Records Disposal Schedule, Oral Health Services, Department of Health (No. 2017/3)* *Records Disposal Schedule, Patient and Client Medical Records, Department of Health (No. 2022/003)*

Queensland	*Public Records Act 2002*	*Births, Deaths and Marriages Registration Act 2023*	*Health Sector (Clinical Records) Retention and Disposal Schedule 2021*
South Australia	*State Records Act 1997*	*Births, Deaths and Marriages Registration Act 1996* *Public Sector (Data Sharing) Act 2016* *Right to Information Act 2009*	*General Disposal Schedule No. 28: Clinical and Client-Related Records of Public Health Units in South Australia 2014*
Tasmania	*Archives Act 1983*	*Births, Deaths and Marriages Registration Act 1999* *Right to Information Act 2009*	Office of the State Archivist, Disposal Schedule for Functional Records of Health Administration 2023
Victoria	*Public Records Act 1973*	*Births, Deaths and Marriages Registration Act 1996*	Disability Services Functions, Retention & Disposal Authority: PROS 08/13, Public Record Office Victoria Higher and Further Education Functions, Retention & Disposal Authority: PROS 16/07, Public Record Office Victoria

		Freedom of Information Act 1982 *Victorian Data Sharing Act 2017*	Public Health Functions, Retention & Disposal Authority: PROS 08/15, Public Record Office Victoria Patient Information, Retention & Disposal Authority, PROS 11/06, Public Record Office Victoria Statewide Health Service, Retention & Disposal Authority, PROS 12/05, Public Record Office Victoria
Western Australia	*State Records Act 2000*	*Births, Deaths and Marriages Registration Act 1998* *Freedom of Information Act 1992*	*Patient Information Retention and Disposal Schedule for the WA health system 2019* *Western Australian University Sector Disposal Authority 2023*

Table 4: Document retention requirements for different types of state and territory records that are used in clinical trials

State or Territory	Record Type	Disposal Requirements
Australian Capital Territory	External or internal reports evaluating the programs and services provided to patients in hospitals, health centres, clinics or other similar health care facilities that cause a change to policies, procedures or is a significant program, unusual item, system or a first time service Records documenting major research carried out relating to population health care management and control programs and strategies	Retain as Territory Archives
	Records relating to the conduct of clinical research, including recruiting and consent of participants, collection and analysis of data, preliminary findings, surveys and results	Destroy 15 years after last action or date of publication of the research, whichever is later
	Records documenting routine research carried out relating to population health care management and control programs and strategies	Destroy after 10 years
	Records relating to clinical trial projects submitted to Human Research for approval The management of join ventures relating to population health care management and control programs and strategies Records relating to the conduct of non-clinical research, including records related to the collection of data, data analysis, preliminary findings, surveys and results Health records about a health consumer	Destroy after 7 years

	Records relating to clinical and non-clinical research where research did not proceed	Destroy after 3 years
New South Wales	Records relating to the conduct of clinical research Records relating to successful applications for approval of clinical research projects	Retain minimum of 15 years after date of publication or completion of the research or termination of the study
	Records relating to the conduct of non clinical research Records relating to approved applications for non clinical research projects	Retain minimum of 5 years after date of publication or completion of research
	Records of requests relating to projects where the research does not proceed Records relating to applications that were not approved	Retain minimum of 3 years then destroy
Northern Territory	Records documenting Centre for Disease Control research data, including raw data	Retain in organisation
	Clinical Research – gene therapy Final research reports in relation to national critical care and trauma response Final versions of clinical research reports in relation to oral health services Final original research in relation to alcohol and other drug services	Retain and transfer to archives service 10 years after action completed
	Clinical Research – non-gene therapy	Destroy 15 years after last access
	Records documenting draft versions of research reports	Destroy 15 years after action completed

	Research data in relation to oral health services	Destroy 10 years after action completed
	Research data for reference purposes	Destroy when reference ceases
Queensland	Any record related to incidents, allegations, disclosures and investigations of abuse of vulnerable people.	Retain for 100 years after creation of record
	Clinical research records where the patients/clients or subjects were adults, including clinical questionnaires and surveys, laboratory results and consent forms	Retain for 15 years after completing clinical trial or after date of publication or termination of study AND 10 years after last patient/client service provision, whichever comes later
	Clinical research records where the patients/clients or subjects were minors	Retain until patient/client attains 18 years of age AND for 15 years after completing clinical trial or after date of publication or termination of study AND 10 years after last patient/client service provision, whichever comes later
South Australia	Records relating to the screening of applications, including approval or rejection of applications by human research ethics committees Records relating to the evaluation of significant public health unit research programs	Permanent
	Informed consent records Participant recruitment records All research data, including electronic data Records relating to evaluation of minor public health unit research programs Research practice activities	Destroy 15 years after research project completed

Tasmania	Records of continuing value documenting publicly funded research and clinical trials, including summary records of research proposals and detail records of research projects or clinical trials	Retain as state archives
	Medium-term records of research and clinical trials, including agreement and contract registers, contracts and agreements, and records of establishment, membership and abolition of controlling committees/authorities for joint ventures entered by hospitals or health services for research or clinical trials	Destroy 15 years after action completed
	Short-term records documenting the management of publicly funded research and clinical trials	Destroy 15 years after action completed
Victoria	Research findings on chronic disease prevention which are of interest to the community or lead to changes in legislation or agency policy Research outcomes that result in changes to policy, practice or new programs relating to health services Research reports developed to establish best practice within an area and to inform policy and program development	Retain as State Archives
	Research findings on chronic disease prevention which are of a more routine nature and do not lead to changes in legislation or agency policy Research outcomes that do not result in changes to policy, practices or new programs relating to health services	Destroy 15 years after administrative research has concluded
	Research data, data analysis, preliminary findings and surveys collected for research into preventing chronic disease	Destroy 15 years after research is published

	Research that facilitate the development of research reports, including statistics and raw data	
	Health information relating to an individual who is 18 years or older	Destroy after 7 years
	Research data and datasets created as part of research activities which involve minors	Destroy 15 years after the child reaches the age of 18. See Retention & Disposal Authority: Pors 16/07, 3.3.4
	Consent forms	Depends on the nature of the treatment provided. See Retention & Disposal Authority: Pros 11/06, 2.1 to 2.4
Western Australia	Records of major research that involves gene therapy Research data from major research involving gene therapy Ethics clearances for major research involving gene therapy	Retain 5 years after date of publication or completion of project, then transfer to State Records Office
	Records of minor research that involves clinical trials Minor research data that involves clinical trials Ethics clearances for minor research that involves clinical trials	Destroy 15 years after date of publication or conclusion of project
	Records of minor research that involves children Minor research data that involves children Ethics clearances for minor research that involves children	Destroy 7 years after date of publication or conclusion of project or after the subjects have reached 25 years of age, whatever is later
	Records of minor research that is not covered by other minor research classes Minor research data that is not covered by other minor research classes	Destroy 7 years after date of publication or conclusion of project, whichever is later

	Ethics clearances for minor research not covered by other classes	
	Unsuccessful applications for ethical clearance	Destroy 2 years after action completed
	Research data where consent for use has been withdrawn by the participant	Destroy after notification of withdrawal

Table 5: Breakdown of requirements for a waiver of consent under Commonwealth, state and territory privacy and health information laws

Jurisdiction	Use or disclosure of health information for research	Use or disclosure of personal information other than health information for research
Commonwealth	The use or disclosure of health information is necessary for research relevant to public health or public safety, and it is impracticable to obtain consent. The research must also comply with guidelines issued by the NHMRC (including the National Statement on Ethical Conduct in Research) and therefore must be approved by a human research ethics committee (HREC) (*Privacy Act 1988* (Cth) s 16B(3)).	No research exception for personal information in the *Privacy Act 1988* (Cth).
Australian Capital Territory	The use or disclosure is necessary for research in the public interest, it is impracticable to obtain consent and the information is de-identified (*Health Records (Privacy and Access) Act 1997* (ACT), Schedule 1, s 10(3)).	No specific research exemption for personal information in the *Information Privacy Act 2014* (ACT)
New South Wales	The use of the information is reasonably necessary for research in the public interest, and it is impracticable to obtain consent or reasonable steps are taken to de-identify the information. The research must also comply with guidelines issued by the Privacy Commissioner. These guidelines require research involving humans to be approved by a HREC in accordance with the National Statement (Dickie, 2004, pp. 13-22).	The use of the information is reasonably necessary for research in the public interest, and it is impracticable to obtain consent or reasonable steps are taken to de-identify the information. The research must also comply with guidelines issued by the Information and Privacy Commission. These guidelines require research involving humans to be approved by a HREC in accordance with the National Statement (Coombs, 2019, para. 2.2).
Northern Territory	The use or disclosure is in the public interest, no individual will be identified, it is impracticable to obtain consent, and the provider of the health information reasonably believes the recipient will not disclose the information. The research must also comply with the Information Commissioner's Guidelines (*Information Act 2002* (NT) schedule 2, s 2.1(ca); s 86(1)(a)(iv)). These guidelines require	The use or disclosure is in the public interest, the research uses personal information in a de-identified form, it is impractical to obtain consent and it is reasonably believed the recipient will not disclose the information (*Information Act 2002* (NT), schedule 2, clause 2.1(ca)).

	research to be approved by a HREC in accordance with the National Statement. The Chief Health Officer (CHO) of the Northern Territory may also authorise the use or disclosure of health information if it takes steps to protect the privacy of persons to whom that information relates (*Public and Environmental Health Act 2011* (NT), s 112(3)).	
Queensland	The use or disclosure is necessary for public health or safety research, it is impracticable to obtain consent, is conducted in accordance with guidelines approved by the Chief Executive of Queensland Health and the agency reasonably believes the information will not be disclosed further (*Information Privacy Act 2009* (QLD) schedule 4, clause 4). Queensland Health procedures require approval by a HREC. Health information can also be disclosed pursuant to Chapter 6, Part 4 of the *Public Health Act 2005* (QLD).	The use or disclosure is necessary for research in the public interest, the information is in a de-identified form and seeking consent is impracticable (*Information Privacy Act 2009* (QLD) schedule 3, clause 6.3(g)).
South Australia	Personal information collected by a person engaged or formerly engaged with the South Australian health system can be disclosed for research if the research methodology has been approved by an ethics committee and there is no reason to believe the disclosure would be contrary to the person's best interests (*Health Care Act 2008* (SA), s 93(3)(f)). Personal information collected for public health purposes can be disclosed for medical, research or statistical purposes if there is no reason to believe disclosure would be contrary to the person's best interests and the Chief Public Health Officer approves the disclosure (*Public Health Act 2011* (SA), s 99(2)(i)).	No specific research exemption in the Information Privacy Principles Instruction (2020)
Tasmania	The use or disclosure is for research relevant to public health and safety, it is in de-identified form, it is impracticable to obtain consent,	The use or disclosure is necessary for research or statistics in the public interest, does not identify any individuals and the agency

	and the information is collected as required by law by competent professionals (*Personal Information Protection Act 2004* (TAS), schedule 1, s 10(4)). Disclosure of public health information can also be authorised for approved study or approved research (*Public Health Act 1997* (TAS), s 147(3)(f)).	reasonably believes the recipient will not disclose the information (*Personal Information Protection Act 2004* (TAS), schedule 1, clause 2(c)).
Victoria	The use or disclosure is necessary for research in the public interest, it is impracticable for the organisation to seek consent and the information is in a de-identified form. The use or disclosure must also be in accordance with guidelines issued by the Health Complaints Commissioner (*Health Records Act 2001* (VIC), schedule 1, clause 2(g)). These guidelines require all research to be approved by a HREC.	The use or disclosure is necessary for research in the public interest and it is impracticable for the organisation to seek consent (*Privacy and Data Protection Act 2014* (VIC), schedule 1, clause 2.1(c)).
Western Australia	Health information may be disclosed by the CEO of the Department of Health if disclosure is reasonably necessary, the purpose for which the information is to be disclosed cannot be achieved without personal information and it is impracticable to obtain the consent of the individual to whom the information relates. The information must also be approved by a HREC (*Health Services Act 2016* (WA), s 216; *Health Services (Information) Regulations 2017* (WA), regulation 3)	The use or disclosure is necessary for research or the compilation of statistics, the research or statistics are not published in a form that identifies the individual and it is impractical to seek consent or the entity disclosing the information believes the recipient will not further disclose the information (*Privacy and Responsible Information Sharing Bill 2024* (WA), schedule 1, clause 2.1(c)).

Appendix 3: Data Glossary

Term	Definition
Aboriginal Health Research Ethics Committee	A specialised HREC that reviews human research with Aboriginal or Torres Strait Islander participants or communities.
Administrative data	A data collection made up of information that is routinely collected during the delivery of a service. These data are collected via departments and agencies and used for policy, planning, management, monitoring, evaluation and research purposes. These data are not typically collected for research purposes but may be used for clinical trials or future research using clinical trial datasets.
Adverse event	Any unfavourable medical occurrence in a trial participant administered the investigational product. The adverse event does not necessarily have a causal relationship with the treatment.
Aggregate data	Data that has been grouped together so it no longer identifies specific individuals. 'Aggregate data' is sometimes used interchangeably with 'summary data' or 'tabulated data'.

Bundled Consent	A bundled consent is a single request from an individual, organisation or agency that includes several requests within it to collect, use and disclose someone's personal information. It does not let the person to whom the information relates, choose which requests they consent to and which they do not.
Capacity	The ability of a person to consent to a clinical trial, research or other forms of medical procedure. A person has decision making capacity if they can understand the information relevant to the decision, retain that information to decide something, weigh that information as part of a decision-making process and communicate that decision.
Cell size	The number of cells (rows or columns) in a dataset that all share a particular value. Where this cell size is small, de-identification should be applied to the data to reduce disclosure risks.
Clinical trial	Any research study that prospectively assigns human participants or groups of human participants to one or more health-related interventions to evaluate the effectiveness on health-related outcomes.
Clinical trial dataset	A dataset collected or generated during a clinical trial.

Clinical trial protocol	A plan that explains the purpose and procedure of the clinical trial protocol. This may include the rationale, design, methodology for the trial, inclusion and exclusion criteria, the length of the trial, procedures, methods of analysis, and safety/quality monitoring.
Clinical trial research agreement	A legally binding agreement that governs the relationship between a sponsor and the institution that is responsible for the conduct of the trial.
Cloud Computing	Computing infrastructure and applications that are available over a network. Cloud computing services are typically scalable to meet demand. This term may be used interchangeably with ‘cloud environment’.
Confidentiality, Duty of	A legally enforceable obligation to maintain the confidence of certain information. This obligation can apply to an individual, an organisation, an agency or the officer of an agency.
Consent	An expression of a person’s willingness to participate in a particular activity. Consent must be informed, voluntary, specific and given by a person with decision-making capacity or their guardian.

Consumer Group	A group or organisation that represents people who use health services or carers for people who use health services. Representatives of these groups may provide consumer perspectives, contribute consumer experiences and take part in decision making processes. This term is synonymous with ‘participant groups’.
Data Asset	A data set that is formally recognised and governed by a data custodian. The terms ‘data collection’ or ‘data holding’ are sometimes used interchangeably with ‘data asset’. A data asset may be collected or created internally by an organisation, gathered through a survey, obtained from or held by one or more government agencies, or merged from several data sets.
Data Linkage	The process of joining or linking together two or more data sets because they refer to the same entity (such as the same individual or institution). This term is sometimes used interchangeably with ‘record linkage’ or ‘data integration’.
Dataset/Data Set	A collection of structured data in a single file or repository.
Data Breach	Where a dataset is accessed, modified, used, disclosed or misused by an entity that does not have authority to access that data.

Data Custodian	Any entity, including a person, agency or organisation, responsible for managing the use, disclosure and protection of data in a dataset. A data custodian may also be responsible for ensuring the dataset adheres to quality and security standards. The term ‘data custodian’ may be used interchangeably with ‘data steward or ‘data access committee’ (depending on the size of the dataset).
Data Sharing Agreement	A legally binding arrangement between a data custodian and another agency, organisation or individual that specifies how a dataset may be shared and used.
Data Sharing Policy	A policy that addresses the types of data held by a data custodian, the principles and strategy around the sharing of that data and the governance and management procedures that should be adopted when this data is being shared.
Data management plan	A document that addresses how data and information will be generated, collected, accessed, used, analysed, disclosed, stored, retained, disposed of and shared, as well as the risks associated with these activities, and any strategies for minimising those risks.

Data repository	The final location where data will be published or stored at the conclusion of a research project. A data repository can either be a subject or domain specific repository, an institutional data repository or a generalist repository.
Data retention	The storage of data for archiving or auditing purposes at the end of a research project.
Data security	The use of strategies to protect data from disclosure risks, alteration and destruction.
Data sharing	The process of making data available to another person, agency or organisation.
Data storage	When an agency, organisation or person physically holds or otherwise controls data.
De-identification	The process of removing identifying details from a dataset so that it no longer contains identifiable information. This can involve multiple processes, including aggregating data or applying privacy enhancing technologies. De-identification should be understood more as a process rather than an output. The appropriateness of different de-identification techniques will depend on the setting in which the data is made available, as well as who is performing the de-identification process.
Disclosure risk	The likelihood that an individual may be re-identified from a dataset. This is sometimes synonymously referred to as an identifiability risk.

Direct personal identifier	A value that can be used to identify an individual without being combined with any other value. A direct personal identifier could include a name, an address, a postcode, a full date of birth or a unique personal identifier such as a Medicare number.
Dynamic consent	An informed consent framework where participants can adjust their consent choices for different research projects over time. This framework is given effect through a technological platform.
Electronic health record	An individual health record for a person stored in an electronic platform that is accessible by their health care team. This term is sometimes used interchangeably with ‘electronic medical record’ or ‘electronic patient record’.
Ethical approval	A determination by an ERB that a research project is ethically acceptable and in accordance with relevant standards and guidelines.
Ethics review	A process conducted by an Ethics Review Body to ensure that research has scientific merit, the benefits outweigh any risks, the research team are appropriately qualified, and respect is shown for the participants.

Ethics Review Body	A body that is responsible for assessing the ethical merit associated with a particular research activity. This definition can include but is not limited to human research ethics committees and low risk ethics review panels.
Extended consent	Consent by a participant for the use of their information for future research projects that are closely related to the original research project or in the same area of research.
Free Prior and Informed Consent	A framework for consent when working with Indigenous communities that understands consent as an agreement concluded without coercion or undue pressure. Under this framework, an individual should have clear mechanisms to modify or withdraw their consent at any time.
Guardian	A person with legal authority to make decisions on behalf of another person.
Health information	Personal information about the health of an individual, what healthcare they have received or might want in the future, as well as information about organ donation or genetic information.
Health related interventions	Surgical treatments, pharmacological treatments, the use of medical devices or other therapeutic goods, preventative strategies or education campaigns.

Human Research Ethics Committee (HREC)	A body registered with the NHMRC to review whether a research project is ethically acceptable and in accordance with relevant standards and guidelines.
Indigenous Data Sovereignty	The right of Indigenous people to govern the collection, ownership and use of data about Indigenous communities, peoples, lands, cultural knowledge, and resources.
Indirect personal identifier	A value that may be combined with other values to identify individuals from a dataset. These values could include age, ethnicity, sex, marital status, occupation, height or weight. These values could also be included in images, such as MRI scans and X-rays.
Investigator	A researcher or other person who is responsible for the conduct of a clinical trial and managing participants. Where there are multiple investigators attached to a clinical trial, the lead investigator is referred to as the principal investigator.
Law	Legislation or a common law decision that is legally binding in Australia.
Legislation	A law made by the Commonwealth Parliament of Australia, or a state and territory Parliament.
Low risk research	Research in which there is no risk of harm, but in which there is a risk of discomfort and in which there may also be a foreseeable burden.

Metadata	Any data about a dataset. In the context of a clinical trial, metadata includes any data variable labels, as well as the clinical trial protocol , the statistical analysis plan or any code generated during the trial.
Minimal risk research	Research where there is no risk of harm or discomfort, but only a potential for minor burden or inconvenience for participants.
Non-Identifiable Data	Data that has been rendered non-identifiable so it is impossible without legal or technical means to re-identify the data.
Opt-out approach	A method used in the recruitment of participants into research where information is provided to the potential participant regarding the research and their involvement and where their participation is presumed unless they take action to decline to participate.
Participant	An individual who participates in a clinical trial.
Participant Information and Consent Form	A form which provides participants with information about a clinical trial, such as the trial's purpose, duration, interventions, risks and potential benefits. The form also allows participants to provide informed consent to participate in the trial.

Participant-level data	Any raw data collected or generated about participants. This data can include any tests conducted on participants, any care or diagnosis received by participants or any adverse events experienced. Direct personal identifiers are usually removed before sharing the data.
Personal information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable.
Private sector organisation	A natural or legal person that is not a federal government agency, or a state or territory government agency. In the context of clinical trials, a private institution could include a private research organisation or hospital.
Privacy enhancing technologies	Technical measures that are designed to reduce the risk of individuals being re-identified from a dataset. The term ‘privacy enhancing technologies’ is sometimes used interchangeably with ‘privacy-preserving techniques’.
Quality improvement	An activity involving a healthcare system that will lead to better patient outcomes, system performance or professional development. Quality improvement should be treated as a separate activity to research.

Quasi-identifiers	A value associated with a dataset that does not identify an individual on its own but when combined with other data, could be used to re-identify individuals from that dataset. The more quasi-identifiers for each record in a dataset, the more likely that they could be used to identify individuals from these records.
Rare disease	A disease that affects less than five in 10,000 people.
Regulation	Any attempt to achieve a publicly stated objective or set of objectives, including but not limited to guidelines issued by a government department or public agency.
Research	Any activity undertaken to gain knowledge and understanding.
Regulatory agency	A body that has the power to investigate a clinical trial or research project. Relevant regulatory agencies for clinical trials in Australia include but are not limited to the Therapeutic Goods Administration (TGA), the Office of the Australian Information Commissioner (OAIC), and any state or territory privacy regulators.
Re-identifiable data	Data where individual identifiers have been replaced with a code or pseudonym. Individuals in the dataset can be re-identified using that code, or if the dataset is combined with another dataset.

Reproducibility	The ability to analyse existing data from a previous study to verify the study's findings or uncover potential concerns.
Risk	The likelihood of a particular event (either positive or negative) occurring.
Secondary research	Research where existing data is used to answer new research questions, validate findings or inform policy and practice. This research must be separate from the original purpose for which the data was collected or generated.
Secondary use	Uses of data for a purpose other than that for which it was specifically collected. Secondary uses can include developing or improving health services or products, developing government policy, evaluating health programs, recruiting participants for clinical trials and conducting research.
Sensitive personal information	Any personal information about an individual's racial or ethnic origin, political opinions or membership of a political association, religious or philosophical beliefs, membership of a profession, trade association or trade union, sexual orientation, criminal record. Sensitive personal information also includes health information, genetic information or biometric information used for biometric verification or identification.
Specific Consent	Consent by a participant to participate in a specific research activity.

Sponsor	An organisation or consortium responsible for initiating, managing and financing a clinical trial. A sponsor can include a private organisation, a health service organisation or a university.
State government agency	A Minister or Department of a state or territory government of Australia, as well as a body established under state or territory legislation.
Study protocol	A document that describes the objective, design, methodology, statistical considerations and organisation of a clinical trial. The term ‘study protocol’ may be used interchangeably with ‘clinical trial protocol’ or ‘protocol’.
Trusted Research Environment	A computing environment that allows researchers to remotely access and analyse a dataset without the dataset leaving that environment or the researchers being able to link it with other datasets. This may be used synonymously with ‘secure research environment’ or ‘secure remote access’.
Unspecified consent	Consent to use a participant’s personal information for any future research project.
Value	An attribute associated with the records in a dataset.
Verification	The process of independently assessing any evidence collected or generated.

Waiver of the requirement for consent	Authorisation for a research team to undertake research without the consent of study participants. In Australia, a waiver of the requirement for consent may be authorised by an ERB. For personal information in medical research, or personal health information, a waiver must be authorised by a human research ethics committee.