TITLE	Cabrini Research Data Management, Access and Sharing Policy
SETTING	All staff, honorary appointments, VMOs, and students engaged in research (or research support) at Cabrini Health - All sites engaged in research, or research support

PURPOSE

Cabrini Health acknowledges that high quality research and data output can only result from high data quality. Data quality encompasses data integrity, accuracy, and validity. Proper data management is crucial to maintain scientific rigor and research integrity.

Patient data confidentiality is both a legal and ethical obligation.
The purpose of this policy is to outline those obligations, the roles, and responsibilities of staff members, VMOs, students and any other personnel involved in collecting, handling, accessing, or sharing research data. This policy has been developed to foster best practice around data management including relevant ethical guidelines, privacy legislation and guidelines, and relevant laws and regulations.

SCOPE

This policy applies to research data managed at Cabrini Health by Cabrini Staff (including honorary, affiliates and associates) and students. It applies to all media of data collection and storage, including, but not limited to paper-based data collection forms, excel spreadsheets, online databases, and registries. It also encompasses all research data generated, collected or used at Cabrini Health including publicly available data, health data or sensitive data.

ROLES AND RESPONSIBILITIES

Data Custodian: individual(s) that is responsible for the implementation of identified business rules for secure access, transport, storage, disposal and availability of data.

Data Owner: Principal Investigators and / or researchers conducting the project are the Data Owners of collated and aggregated research data as part of the research project and to be defined in each research project protocol and associated Data Management Plan. Patients are ultimately the Data Owner of their own individual Data.

Data Steward: individual(s) who control the data and is/are responsible for the definition, quality, and maintenance for end-to-end usage of the business data in their area of responsibility, generally defined by a data subject area.

Database Manager: individual that is responsible for overseeing the acquisition, validation, storage, protection and processing of sets of data, and compliance with approved national guidelines.

Data Governance Committee: this committee has been established to oversee all activities related to databases and registries involving Cabrini patients. It will establish clear guidelines for all activities in relation to the databases and registries, creating a uniform approach throughout the institution. This Committee is acting as the custodian for Cabrini Health research-related activities.

Principal Investigator: retains the responsibility at the Cabrini site and maintains appropriate supervision of any delegated study specific persons or parties undertaking the activities to ensure the rights, safety and wellbeing of the study participants and data reliability (ICH GCP).

DEFINITIONS

Data: factual information used as a basis for reasoning, discussion or calculation in digital form that can be transmitted or processed.

Data Governance: specifies a cross-functional framework for managing data as a strategic enterprise asset. In doing so, data governance specifies decision rights and accountabilities for an organisation in its decision-making about its data. Furthermore, data governance formalizes data policies, standards and procedures, and monitors compliance[1].

Data Management: implementing, enacting and making data governance decisions part of the day-to-day processes throughout the data lifecycle.

Data Management Plan (DMP): a written document describing how the project team members expect to capture, generate, collect, audit, clean, store and use research data. It also describes the mechanism and processes used at each step of the data lifecycle and security measures in place.

De-identified Data: as defined in the Privacy Act 1988, as personal information that is no longer about an identifiable individual or an individual who is reasonably identifiable.

Health information: subcategory of personal information, defined in the Privacy Act 1988 as:

- information or an opinion about:
    - the health, including an illness, disability or injury (at any time) of an individual; or
    - an individual's expressed wishes about the future provision of health services to the individual; or
    - a health service provided, or to be provided, to an individual; that is also personal information; or
- other personal information collected to provide, or in providing, a health service to an individual; or
- other personal information collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or
- genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual.

Identifiable data: data that enables the identification of a specific individual.

Metadata: a set of data that provides information about other data. It is used to summarise basic information about data making tracking and working with specific data easier.

Non-identifiable data: data that has never had identifiers collected with or attached to it, or has had all identifiers permanently removed. Re-identification of the person to whom the data relates to is not possible.

Personal information: information is defined in s6(1) of the Privacy Act as: "information or an opinion about an identified individual, or an individual who is reasonably identifiable:

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

Potentially identifiable (coded, re-identifiable) data: is data that may have identifiers removed and replaced by a code. In such cases it is possible to use the code to re-identify the person to whom the data relates, that is, the process of de-identification is reversible.

[1] Abraham R, Schneider J, vom Brocke J. Data governance: A conceptual framework, structured review, and research agenda. International journal of information management. 2019;49:424-38.

Sensitive Information: is defined in the Privacy Act 1988 as meaning:

- information or an opinion about an individual's:
  - racial or ethnic origin; or
  - political opinions; or
  - membership of a political association; or
  - religious beliefs or affiliations; or
  - philosophical beliefs; or
  - membership of a professional or trade association; or
  - membership of a trade union; or
  - sexual orientation or practices; or
  - criminal record;

that is also personal information; or

- health information about an individual;
- genetic information about an individual that is not otherwise health information; or
- biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
- biometric templates.

Secondary Use of Data: access to and use of data that was originally generated or collected for previous research or non-research purpose.

POLICY

This policy follows the Australian Code for the Responsible Conduct of Research (The Code) as well as its *Management of Data and Information in Research* supporting guide. The following principles are relevant to the management, access and sharing of data:

- Principle 2, 'Rigour in the development, undertaking and reporting of research', which requires that research be characterised by attention to detail and robust methodology and that researchers avoid or acknowledge biases.
- Principle 3, 'Transparency in declaring interests and reporting research methodology, data and findings', which requires researchers to share and communicate research methodology, data and findings openly, responsibly and accurately.
- Principle 7, 'Accountability for the development, undertaking and reporting of research' so as to comply with relevant legislation, policies and guidelines and ensure good stewardship of public resources used to conduct research.

The responsible conduct of research includes the generation, collection, access, storage, analysis, disclosure, retention, disposal and sharing of data and information. All of these steps are key elements in maintaining research and data integrity throughout the data lifecycle. Managing research data appropriately helps:

- Save time through efficient and accurate data collection, handling and processing;
- Minimise risks of accidental data loss, disclosure or theft and intellectual property disputes;
- Retain integrity and ensures research output is reproducible;
- Comply with funding agencies and publisher's requirements of making research data available.

Further to The Code's principles, Chapter 3 element 4 of the National Statement on Ethical Conduct in Human Research (2023) provides guidance on collection, use and management of data and information including identifiability of information, secondary use and sharing of data or information. It should be read in conjunction with this policy and all other relevant legislation and guidelines, including the Health Record Victoria (2001), the Privacy Act 1988, in particular the Guidelines under Section 95 as well as the related 13 Australian Privacy Principles.

Data Lifecycle:

Data management is a central element at each of the data lifecycle steps including the planning, capture, curation, analysis, sharing and dissemination, archiving and re-use of the data as per the figure below.

Figure 1. Data lifecycle from research planning through to archiving. Data storage and management underpin the entire lifecycle.

Research Planning: in this initial step researchers need to plan what data needs to be collected from intended sources to answer the research question and start the planning for the data throughout the project. While deciding upon what data should be collected, the participant's privacy should remain at the forefront. All the data required to answer the research question should be captured, but not beyond what is required, thus minimising excess data collection and increased data privacy risk for participants. An example of this is to collect year of birth rather than full date of birth. During this first stage a data management plan (DMP), should be created (see more details below). Spending time in this planning and design phase will greatly increase efficiencies in the next step of the data lifecycle.

Capture and Curation: This step of data collection, potentially from various sources, can be a very time consuming but can be optimised by careful planning during the Research Planning step. High quality data is achieved by collecting data from the source of truth. Data curation, ie cleaning and auditing, is a key process to ensure data is of the highest quality. When collecting data from multiples sources, quality audit and standardisation are of the upmost importance to ensure that the data collected is accurate, valid and reliable.

Analysis: The data analysis step is facilitated through carefully considered design planning at the start of a research project and should be performed in accordance with the planned statistical analysis. It is encouraged to involve Cabrini's biostatistical services (biostats@cabrini.com.au) in the research planning stage to optimise the data analysis stage. Data analysis can be done as part of a collaboration, provided the required agreements are in place.

Sharing: Sharing of research data can happen at various points throughout the data lifecycle. Before any data sharing can be performed, researchers always need to ensure the sharing of data is ethically and legally allowed and that all required agreements and data safeguards are in place. See more details on data sharing below.

Dissemination: Dissemination of research data outputs can be in various forms from peer review publication to conference presentations or scholarly products. Before publishing, researchers are required to ensure the publishers' data sharing requirements are understood and can be complied with. Cabrini staff are also expected to comply with the *Cabrini Authorship and Publications for Research Policy* when disseminating research outputs.

Re-use: Data re-use is using data for other purposes than it was originally collected for. Data re-use is an essential component of research as it avoids doing repetitive and unnecessary studies. It also promotes repeatability and research robustness. Prior to re-using data, verify that the data has been ethically collected and the reuse conditions conforms with policies and regulations.

Retention & Archiving: Archiving data means moving data that is no longer actively used to a separate storage location for long-term retention. This is distinct from data backup, which is making a copy of actively used data and storing it in a separate location for the purpose of restoration in the event of loss or damage of original data.

Store and management: Storage and management of research data underpins the entire data lifecycle. Data management is effectively a risk management exercise and should not be static but rather be continuously checked and updated to ensure data is securely stored and the data management plan is adhered to. For data storage guidance, please refer to the *Data Classification and Labelling Standard - Cabrini*.

Data Management Plan and Data Dictionary:

A Data Management Plan (DMP) should be developed as early as possible in the design of a research project and alongside a study protocol. It should provide the details on how data will be handled throughout the study and should be reviewed regularly throughout the lifecycle of the research data. Each study or research project should have its own DMP.

A DMP should address the following points:

- Description of the study data – this section should include details on what data or information is required to achieve the aims of the research project, including (but not limited to) sample size, type of data collected (qualitative or quantitative), data sources and formats; the purposes for which the data will be used and disclosed.
- Data generation, collection and capture – this section should include details of how and by whom data will be generated or collected, and what instruments or tools will be used. For example: data collected by the database manager using a paper or online survey, excel spreadsheet or electronic data capture tool, data import or manual data collection, etc. Access permissions and the level of identifiability of data for each study team member should be clearly stated. The form in which the data will be stored should also be described in this section, as well as retention periods and disposal plans.
- Data security – this section should describe the measures put in place to safeguard the data and the patients. This should include back up methods (including disaster recovery), and the physical, network and technical security measures in place.
- Analysis and reporting – this section should refer to the statistical analysis plan of the study protocol and describe any plans to report the data, such as publications, annual reports, and other public facing forums. This section should also state how and by whom the data will be used and analysed.
- Data Access and Sharing plan – this section should state any planned or expected data sharing activity, external data transfers and data linkage activities. It should also list the conditions under which the data will be shared or how access to the data is granted to others. This should include considerations around the Australian Privacy Principles (APPs), HREC approval and any other relevant legislation and laws. See section below for further details.

- Roles and responsibilities – this section should summarise the roles and responsibilities of each study team member undertaking the research project. Ensure that roles are covered by multiple team members to ensure redundancy in case a team member where to leave Cabrini Health.
- Risk – unless already thoroughly addressed in the research protocol, risk and severity of any harm associated with or resulting from the collection, use and management of the data should be described in this section as well as how risks can be minimised.

The DMP is preferred as a separate document to the protocol but can also be included as a clearly defined section of the study protocol.

Complementary to a Data Management Plan, Data Dictionaries are a key document that ensures good data governance and high-quality data collection. A Data Dictionary is a living document that is version controlled and is to be updated regularly throughout the lifetime of the research project. Its purpose is to list and explain all the data elements to be collected and used to measure the outcomes. Data Dictionaries can be presented in various formats (excel spreadsheets, word documents, etc) and should address the following points (at a minimum) for each data element :

- The name and definition of the data element
    - These should be referenced, wherever possible, to existing data dictionaries/ vocabularies such as METEOR, FHIR-AU, SNOMED-CT, ICD-10-AU, discipline-specific reference sets
- The purpose of collecting that data element
- Database variable/ field names and system mechanism (dropdown, checkbox, free text, etc)
- Permissible values including ranges, code sets
- Relationships between various fields such as:
    - Conditional relationships
    - Derived or calculated values
- Designated data elements that are mandatory and/ or allow an unknown or not stated response.

As part of the Data Dictionary preparation, it is essential to consider if any data elements can be used to identify individuals.

Data identifiability:

Although data identifiability can be referred to as discreet states in various regulations, such as identifiable, re-identifiable, de-identified, non-identifiable (see above glossary for definitions); the identifiability of data is not a suite of distinct and static states but rather can be found on a continuum that is affected by environmental factors as well as where the data is in the lifecycle. Depending on the environment the data is stored in and what other data are available (in the public domain as well as part of the datasets held by the custodian), the identifiability of a dataset might vary and move along the identifiability spectrum. Change in technology can also impact identifiability and can make re-identification of data originally collected or shared in a “de-identified” manner possible.

It is essential to try and reduce the risk of inappropriate identifiability throughout the data lifecycle. Researchers should at a minimum:

- minimise the number of variables collected for each individual;
- separate identifiers and content information, including separation of storage where possible. This includes separation of master key code lists from clinical information of study unique code;
- separate access and permission to identifiers and clinical or content data depending on the roles of each research team member. Access should be sufficient for each team member to perform their roles adequately but restricted enough to not allow superfluous access;
- keep up to date and vigilant to how this data is protected and stored, even if it has undergone a de-identification process as there is always a risk of re-identification.

The data elements listed below can directly or indirectly identify participants:

- Name
- Date of birth or death
- Address (postal or email)
- Phone number
- Social media handle
- Image or photo of face or other unique biometric data or facial recognition biometrics
- Hospital record identifier (URN, MRN)
- Individual Health Identifier (IHI)
- Genetic information
- Medicare / Centerlink identifier
- Signature
- Bank details and Tax File Numbers

In the current age of big data, it is difficult to fully "de-identify" data that is at a person-level, but it is widely agreed that merely removing a person's name, address and other direct identifiers is no longer sufficient (see OAIC advice). The list of direct identifiers is likely to evolve over time and with technological progress.

Direct identifiers should never be shared unless research participants have provided explicit informed consent.

Data Access and Sharing plan:

Granting access to or sharing data originally generated or collected for the purpose of a specific research project or for clinical purposes, is called Secondary Use of data. It is common for data to be collected and stored for an original project and then banked for potential use in future ethically approved research projects. An important ethical issue arising from secondary use of data is the scope of consent provided by participants. Possession, access to medical records or custodianship of data does not mean an automatic right to use it for any desired research purpose. Before any data is used or shared for secondary use of data purposes, the ethical requirements are to be discussed with Cabrini Research Governance Office and all relevant Human Research Ethics Committee ethical requirements approved.

If personal information is to be used or shared, there are further legal considerations. As per the Guidelines under Section 95 of the Privacy Act 1988 (Section 95 Guidelines): the APPs do not permit agencies to use or disclose personal information for medical research purposes, unless the individual has consented to the use or disclosure, or the use or disclosure is allowable through an exception contained in the Privacy Act. Certain exceptions are included in APP 6.2 and 6.3. The Section 95 Guidelines provide a framework for the conduct of medical research using information held or collected by agencies where personal information needs to be used and where it is not practicable to obtain the individual's consent.

Data sharing has become an essential part of research and key step in the data lifecycle. To allow for maximum benefits to be derived from data sharing, the FAIR (Findable, Accessible, Interoperable, Reusable) data principles were developed.

In an ever-increasing need for data sharing and open and transparent research, the Five Safe Framework was developed to balance the risk of disclosure and data utility. Data sharing is a risk management exercise rather than a risk elimination one. The Five Safe Framework takes a multi-dimensional approach to managing disclosure risk, facilitates safe data sharing, and prevents over-regulation in assessing not only the data itself, but also the environment in which it is released.

The Five Safe Framework focuses on the following elements:

- **Safe people:** Is the researcher appropriately authorised to access and use the data? I.e. bone fide researcher, GCP training, confidentiality agreement is in place
- **Safe projects:** Is the data to be used for an appropriate purpose? I.e. HREC approved project, ensure project suitable with data requested
- **Safe settings:** Does the access environment prevent unauthorised use? I.e. IT and environmental conditions of data access and storage are adequate
- **Safe data:** Has appropriate and sufficient protection been applied to the data? I.e direct identifiers have been removed prior to sharing, other protections are in place
- **Safe outputs:** Are the statistical results non-disclosive? I.e. participants cannot be identified in the results or other outputs

The five safe elements put in place need to be commensurate to the data identifiability and amount of details in the data. Aggregated data doesn't require the safe elements to be as stringent as record level identifiable data.

Data Sharing and re-use should be considered from the design stage. A Data Access and Sharing plan should be added to the protocol and should include relevant consent for reuse of the data. Contact Cabrini Research Governance Office for guidance regarding Cabrini's informed consent requirements.

A generic Data Access and Sharing plan should address the following questions:

- **What** data will be shared (e.g.: demographic, molecular profiling, clinical information, survey data, bioassays)? In what format (e.g.: aggregated, record / unit level)?
- **How** will data be shared (e.g.: via secure file transfer, via data access in a controlled environment)?
- What **metadata** will be shared alongside the data?
- Will any **supporting documentation** (e.g.: protocols, data dictionary) be shared with the data?
- **Who** will access or be able to access the data (e.g.: will the data be publicly accessible or will access be restricted)?
- **Where** will the shared data be stored? What are the security processes of the third party the data is shared with? Are the systems and storage secure? Are they compliant with Australian Privacy Principles and other relevant legislation and laws?
- **When** will data be shared (e.g.: prior to or post publication, after an embargo period)?

Data should only be shared if eligible and allowed under the relevant laws and legislation. A Data Transfer or Sharing agreement needs to be signed by all parties prior to sharing any data. Any queries on data sharing agreements can be directed to the Cabrini Research Governance Office researchgovernance@cabrini.com.au .

Data access and sharing for research databases and registries held and managed at Cabrini Health is governed by the Data Governance Committee. If you wish to access or share with collaborators any research data collected, stored and held at Cabrini Health for a project beyond its primary purpose, please contact the Data Governance Committee (email-datagovernance@cabrini.com.au) .
Any outputs generated and published from the data accessed are required to follow the *Cabrini Authorship and Publications for Research Policy* and credit Cabrini Health as per the policy.

Where the sharing of research data has been requested and access has been refused, the reasons for not sharing the data should be transparent and justifiable.

In case the research study involves data linkage, this should also be considered early on in the design process. Some guidance can be found here: National Mutual Acceptance (NMA) Data Linkage.

Indigenous Data Sovereignty:

Beyond the data access and sharing framework listed above, when data is collected about or from First Nations people or about Country, Indigenous Data Sovereignty applies.

Indigenous Data Sovereignty is the right of First Nations people to control data collected about them, their culture and their Country. The CARE Principles have been developed by the Global Indigenous Data Alliance (GIDA) to complement the FAIR principles. While the FAIR Principles are about making it easier to share and reuse data, the CARE Principles ensure that data is used ethically.

The CARE Principles for Indigenous Data Governance are people and purpose-oriented, reflecting the crucial role of data in advancing Indigenous innovation and self-determination[2]. They are focussed on[3]:

- **C**ollective benefits: Data ecosystems shall be designed and function in ways that enable Indigenous people to derive benefit from the data.
- **A**uthority to control: Indigenous peoples' rights and interests in Indigenous data must be recognised and their authority to control such data be empowered
- **R**esponsibility: Those working with Indigenous data have a responsibility to share how those data are used to support Indigenous people's self-determination and collective benefit.
- **E**thics: Indigenous people's rights and wellbeing should be the primary concern at all stages of the data life cycle and across the data ecosystem.

Further information on Indigenous Data Sovereignty can be found in the discussion paper "Taking Control of our Data" from the Lowitja Institute, Australia's national Aboriginal and Torres Strait Islander community-controlled health research institute.

Data Retention and Disposal Requirements:

Research data and relevant primary materials (such as laboratory books, or other research related materials) are to be retained once the research project has been finalised and/or published to be able to justify and defend outcomes of the research in case they are challenged. The Code provides guidelines around minimum retention period of data and recommends treating primary material and data in the same manner.

Data retention is ultimately the responsibility of the Principal Investigator (PI) of each project. The PI decides which data and materials are to be kept. Depending on the type of research the minimum retention period will vary.

Please refer to Table 1 below for data categories and recommended retention periods for Cabrini Health patient research data. The retention period listed in Table 1 is technology agnostic and applies to all types of data and primary materials irrespective of analogue or digital format. If the PI wishes to retain the data and material beyond the minimum retention period, this should be clearly explained in any project documentation including protocol, data management plan and consent forms.

Once the research has been completed, this includes published or abandoned research, the data is to be archived until the end of the retention period. The PI is to contact the IT department to ensure any digital data and primary materials are adequately and securely archived. Any analogue data and primary materials are to be stored in a secure location at Cabrini Health with sufficient and adequate access restrictions. This can be an onsite secure, key or pad locked cabinet, or archived offsite.

[2] https://www.gida-global.org/care

[3] https://ardc.edu.au/resource/the-care-principles/

Table 1: Data retention periods for different research types.

Research type	Data retention period (minimum)
Community, historical or cultural heritage value	Permanently
Subject of controversy or debate	Permanently
Research involving gene therapy	Permanently
Involving the use of major new or innovative technology	Permanently
Clinical trials	15 years for adult patients * And 25 years for paediatric patients* *after completion of trial
Resulting in a patent	7 years after expiry of the patent
General research not falling into any of the other categories	5 years after publication or last action taken including abandoning the research
Quality assurance or assessment (including student project)	2 years after completion

Data and study materials used in research should be disposed of in a manner that is safe, secure, and consistent with the consent obtained and any legal requirements. It is recommended that paper-based data and materials are disposed of using the Secure document destruction bins provided by Cabrini Health.

To dispose of any electronically stored data and materials, please contact the IT department to ensure all files are adequately and fully destroyed.

Storage of consent forms in electronic format

Signed participant consent forms are a component of a project's research material and are required to follow the same guidelines as the rest of the research materials. Storage of signed participant consent forms are required to follow the same guidelines as all other research materials. Digital storage of hard copy consent form (scanned copy) is acceptable provided the following conditions are met:

- Hard copies are disposed of using the confidentiality shred bins provided or other suitable confidential disposal methods.
- Storage, security and retention of the digital copies of the consent forms are to adhere to this policy and any other relevant laws, regulations and guidelines in the same manner as was relevant in the hard copy format.
- Electronic storage is included in the Data Management Plan and submitted to CRGO for review
- Adherence to the *Management of Data and Information in Research: A guide supporting the Australian Code for the Responsible Conduct of Research*

BREACH

In the event a Cabrini staff member suspects or becomes aware of a data breach, they should refer to *the Data Breach Response Plan* to ensure the correct process to identify Eligible Data Breaches (see policy) is followed, potential harm is minimised, and affected individuals and the Office of the Australian Information Commissioner (OAIC) are notified when appropriate. This Plan comprises the procedures consistent with the OAIC guide to managing data breaches in accordance with the Privacy Act 1988. The Privacy Act 1988 requires Cabrini to notify affected individuals and the OAIC of Eligible Privacy Breaches.

As per the *Monitoring of Research Policy*, any serious Breaches are to be reported to the reviewing HREC and CRGO within seven (7) calendar days of confirming a serious breach has occurred. Any actions requested by the reviewing HREC must also be reported to CRGO.

If someone suspects there is research misconduct such as fabrication of data consult with a Research Integrity Adviser at CRGO and/or refer to the *Research Integrity and Misconduct Policy.*

EVALUATION

The effectiveness of this policy will be evaluated by the Data Governance Committee (DGC) with the assistance of the Cabrini Research Governance Office (CRGO).
The Data Management Plan will be reviewed by CRGO and DGC as required and complemented with information requested from researchers as required.
Data access and sharing activities will be directly governed by the DGC.

REVIEW

This Policy shall be reviewed every 3 years or as need arises due to changes in legislation or industry standards. Non-material amendments may be proposed at any time and approved by the Group Director Research.

REFERENCES and ASSOCIATED DOCUMENTS

Cabrini Policies, Procedures and Protocols

Artificial Intelligence (AI) Usage Policy
Cabrini Authorship and Publications for Research Policy
Data Classification and Labelling Standard - Cabrini
Data Breach Response Plan
Monitoring of Research Policy
Research Integrity and Misconduct Policy

Key Legislation and Standards

Privacy Act 1998
Guidelines under Section 95 of the Privacy Act 1988
Australian Privacy Principles
Australian Code for the Responsible Conduct of Research
Management of Data and Information in Research: A guide supporting the Australian Code for the Responsible Conduct of Research
National Statement on Ethical Conduct in Human Research 2023
OAIC Notifiable Data Breach
Health Record Victoria (2001)

References

A-CTEC free course on data management plan
ARDC CARE principles resource
De-identification and the Privacy Act
Five saves framework
National Mutual Acceptance Data Linkage Guide
Taking Control of Our Data discussion paper

Acknowledgements: Cabrini Research Consumer and Community Involvement Committee (CRCCIC)

REVISION HISTORY

Version	Revision date	Revision notes
1.0	16/08/2024	New policy
1.1	21/10/2024	Updated broken Prompt link to listed policies
1.2	04/03/2025	Addition of paragraph on storage and retention of electronic copies of signed participants' consent forms Added reference: Management of Data and Information in Research: A guide supporting the Australian Code for the Responsible Conduct of Research

Document Sponsor	**Group Director Cabrini Research**	
Approved By:	**Data Governance Committee**	**Date:** 16th August 2024
Authorised By:	**Data Governance Committee**	**Date:** 16th August 2024