Research data and privacy

PURPOSE

This work instruction identifies a consistent and enforceable process for the use of confidential health information/research data and privacy for research being conducted in or in collaboration with Metro South Health (MSH).

This work instruction aligns with MSH procedure PR2023-411 Research excellence.

OUTCOME

This work instruction aims to:

- Inform researchers of the correct course of action when requesting health records for research purposes to ensure that patient confidentiality is protected; consistent with evidence-based practice.
    - Note: Patient confidentiality must be protected in the conduct of all research, in line with the ethically approved protocol.
- Outline processes to ensure all research related confidential information/data and MSH records, including primary materials, are stored, disposed of, or transferred in accordance with relevant MSH policies and procedures.
- Ensure privacy is maintained for all MSH patients who participate in research.

This work instruction outlines processes described in MSH procedure PR2023-411 Research excellence and upholds principles outlined within the Research Excellence Handbook.

SCOPE

This work instruction applies to all MSH employees and collaborators who conduct human research within or in association with MSH, or through access to MSH participants, health records or data.

WORK INSTRUCTION

1. STEP 1: DATA REQUIREMENTS AND LINKAGE

- Researchers must consider data collection methods, the types of data required, data linkages required and sources of data when planning and starting a research project.
- As part of planning how the data is collected during the project will be analysed, researchers must also establish a system for organising and managing research project data including:
    - research data management planning
    - storage and security of research data
    - retrieval, retention and record keeping
    - access (i.e., between collaborating researchers/institutes), privacy and confidentiality
    - disposal.

- Once data requirements and sources of data are identified, researchers must detail all aspects pertaining to the management of research data as part of the research protocol.

1.2 Data Custodians

- Based on the research project's requirements, the researcher should identify relevant Data Custodian/s (e.g., Health Information Management Services (HIMS).
    - Note: There may be multiple Data Custodians identified depending on the type of data and linkage requirements.
- Department and facility level activity data is available through the Metro South Data Hub – Safety and Quality – Standard 15.
    - Please confirm with the Metro South Data Hub what documentation is required to support your request (such as Ethics approval/ Waiver of Consent).
- Department of Health – Using confidential information in research provides information when requesting access for Public Health Act (PHA) Information & Application Form and Data Custodian contacts.
- Department of Health – Information sharing also provides useful links and tools to support information sharing.

2. STEP 2: RESEARCH PROJECT DATA RISK ASSESSMENT AND MANAGEMENT PLAN

- Data risk assessment and management in research involves evaluating potential risks associated with the collection, storage, and handling of research data. It aims to identify and mitigate threats to the confidentiality, integrity, and availability of data and helps researchers anticipate and address privacy concerns, data breaches, and other risks to ensure ethical and secure research practices.
- A Research project data risk assessment and management plan (Attachment 1: Research project data risk assessment and management plan) template is available to assist MSH researchers in identifying and assessing the data management risks relevant to the research proposal and what controls are in place/will be put in place to mitigate those risks.
    - Note**:** While the example risks and mitigation examples have been included in the template, these are a guide to identify the potential risks and controls, they are not exhaustive, and researchers may need to consider additional risks or controls depending on their individual proposals.
    - Note: Only complete the Research project data risk assessment and management plan if your project only involves data analysis.
- Not all risks or controls will be relevant to all research proposals and some controls may assist in mitigating multiple risks. Identified controls should be clearly articulated in the protocol.
- MSH work instruction WI2023-292 Assessing and managing risk in research provides further information and guidance around risk assessment in research and can be used to guide in the completion of the Research project data risk assessment and management plan.

2.1 Existing risks and their relevance

- When completing Research project data risk assessment and management plan include any existing risks registered that might be relevant to research risk development for example: Risk #822 Cyber and Information Security.

2.2 Ethical review

- The completed Research project data risk assessment and management plan must be included as part of the Site Specific Assessment (SSA) submitted via the Ethical Review Manager (ERM) application.
- The project data risk assessment can be included as part of the research protocol or as an appendix to the protocol.
- If a waiver of consent is requested and approved, the approving letter from the Human Research Ethics Committee (HREC) must specifically identify this and what data is being approved for release under a waiver of consent.
- MSH work instruction WI2023-299 Ethical and scientific review of research provides further information.

2.3 Reporting

- The researcher must provide an annual and final report on the outcomes of the research to the approving HREC and/or Research Governance Office (RGO) (if multi-site study).
- Researchers must utilise the HREC/RGO Annual Progress Report/Final Report to report on the effectiveness of the data management plan through the lifecycle of the research project.
- MSH work instruction WI2023-306 Post approval – research amendments, reporting and closure provides further information.

3. STEP 3: RELEASE OF CONFIDENTIAL INFORMATION UNDER PUBLIC HEALTH ACT APPROVALS

- Where release of data is approved under the PHA, all information about the application approved by the Director General, Department of Health, Chief Executive Officer, MSH and/or delegate is kept on a Research Registry by the Department of Health (DoH) Office of Research and Innovation (ORI) in accordance with Division 3 s288 *Public Health Act 2005 (Qld)*.
    - Note: This is only required when a waiver of consent has been approved by a Queensland Heath (QH) HREC AND Confidential patient information will be disclosed to third parties (i,e., non-QH entities).
- Researchers must complete the PHA application and email to identified Data Custodian/s for their endorsement of the application.
    - Note: As part of this process, it is important to identify any potential identified barriers with the Data Custodian/s.
- See Appendix 1: PHA application process

3.1 Data Custodian/s endorsement

- Each Data Custodian will email the PHA application back to the researcher with their endorsement (or not).
- The researcher is responsible for collating endorsement from multiple Data Custodians.

3.3 Access to confidential health information – DoH process

- Applications for the release of confidential information/data retained by the DoH for the purposes of research, to a third party under Section 280 of the *Public Health Act 2005 (Qld)* must include:
    - Copy of approval letter from a HREC
    - Evidence of authorisation from the relevant Data Custodian/s
- Researchers must submit PHA applications electronically to PHA@health.qld.gov.au
- Office of Research and Innovation (ORI) will provide feedback on the PHA application and/or grant approval.

3.4 Site specific assessment authorisation

- Researchers must provide a copy of the PHA Approval Letter as part of the Site Specific Assessment (SSA) application via ERM.
- Researchers must receive written SSA authorisation prior to commencement of research or request for health records.
- MSH work instruction WI2023-301 Site specific assessment of research provides information regarding the SSA process.
- Researchers must email the PHA Approval Letter and SSA authorisation to the Data Custodian/s for the ability to access or release data.

4. STEP 4: RELEASE OF CONFIDENTIAL INFORMATION VIA SECTION 150 OF THE HOSPITAL AND HEALTH BOARDS ACT (2011)

- Where release of data is approved under the *Hospital and Health Boards Act 2011* (HHB Act) for the purposes of monitoring, evaluation, planning and delivery, a request can be made to the relevant facilities Health Information Management Unit
    - Logan Beaudesert Health Service: hims_data_LBH@health.qld.gov.au
    - Princess Alexandra Hospital: pah_hims_research@health.qld.gov.au
    - QEII Hospital: qeii_hims_data@health.qld.gov.au
    - Bayside Health Service: himsresearchrlh@health.qld.gov.au

5. STEP 5: PRIVACY

- When collecting, storing, using or disclosing personal information, researchers must abide by the mandatory requirements of the *HHB Act, Information Privacy Act 2009 (Qld) (specifically the nine*

National Privacy Principles (NPPs), MSH policies and procedures pertaining to information privacy and confidentiality requirements.

- Appropriate consent must be gained to access information from data unless the need for consent has been waived by a HREC.
- Consent must be as approved by the relevant HREC and in accordance with the National Statement on Ethical Conduct in Human Research (2023) ('National Statement'), noting in particular, Sections 2, 3 and 4.
- Research projects that seek unspecified future use of personal information must detail the purpose of the information use in the research protocol and the consent form.

5.1 Privacy breaches

- Privacy breaches can occur through various means, often unintentionally. Researchers must be vigilant in protecting the confidentiality and privacy of individuals involved in their studies. Privacy may be breached at various stages of a research project. See below for some examples:
    - Insufficient anonymisation: In a survey, if the collected data is not properly anonymised, it might be possible to trace responses back to individual participants.
    - Inadequate data security: Storing sensitive data on insecure servers or devices, without proper encryption or access controls, could lead to unauthorised access and potential privacy breaches.
    - Inappropriate data sharing: Sharing raw, identifiable data with third parties without obtaining explicit consent from participants can compromise privacy. This includes sharing personal and confidential information electronically or outside of Australia (refer section 33 of the IP Act).
        - Refer to Queensland Health Digital Standard Use of email standard QH-IMP-484-3: 2021.
    - Re-identification risk: Even if data is anonymised, if there are unique or rare characteristics in the dataset, it might be possible to re-identify individuals.
    - Inadequate informed consent: Failing to adequately inform participants about the potential risks and uses of their data can lead to unintentional privacy breaches.
    - Publicly accessible results: Publishing research results that include personally identifiable information without proper redaction can compromise privacy.
    - Data interception: During data transmission, if it is not adequately encrypted, malicious actors could intercept and misuse the information.
    - Surveillance and observation: In observational studies, if participants are not made aware of being observed, it can breach their privacy.
    - Data aggregation: Aggregating data at too granular a level might reveal individual identities, especially in small populations.
    - Invasion of sensitive information: Collecting unnecessary or overly sensitive information that is not relevant to the research goals can be an invasion of privacy.

- Unsecured surveys or interviews: If surveys or interviews are conducted in public spaces without privacy measures, sensitive information may be overheard.
- Inadequate HREC and/or Data Custodian/s review: Example: If a research project is not reviewed and approved, it may lack the necessary safeguards to protect participant privacy.

5.2 Reporting a privacy breach

- If a privacy breach occurs, researchers are expected to address it promptly and appropriately, taking measures to mitigate any potential harm and ensuring that future breaches are prevented.
- In MSH the following process is required:
- The researcher must notify the approving HREC and RGO. If approved in MSH, the contact details are as follows:
  - MSHREC – MSH-Ethics@health.qld.gov.au
  - MSHRGO – MSH-RGO@health.qld.gov.au
- MSH RGO will provide summary level data on a regular basis to the relevant Directorate Research Committees.
- In addition to HREC/RGO notification, the researcher must send an email describing the nature of the incident to the Privacy and Confidentiality Contact Officer.
  a. Decision Maker & Privacy and Confidentiality Contact Officer contacts | Queensland Health
- Note: If a breach occurs, MSH employees must be cautious to avoid breaching again and undertake appropriate remedial actions (e.g., changes to processes or additional training).
- Further guidance regarding privacy and data breaches can be provided by Metro South Research.

5.3 Research integrity

- If there appears to be a breach of the *Australian Code for the Responsible Conduct of Research* 2018 ('the Code'), MSH work instruction WI2023-291 Research complaints and misconduct outlines the preferred model that MSH utilises to investigate and manage potential breaches.
  - Note: A minor privacy breach, on its own, may not necessarily constitute an automatic breach of the Code. The severity of the breach and the context in which it occurs are crucial factors to consider when a concern is identified.

RESPONSIBILITIES

Position	Responsibility	Audit criteria
Executive Management Team	• Review and support/not support data or health record requests through endorsement/non-endorsement of SSA application forms.	N/A
Department/divisional delegates	• Be aware of access to data and/or health records in their departments/divisions.	N/A

	• Maintain local work practices to ensure all researchers are authorised before research health records or data is provided.	
Metro South Research Governance Office (MSRGO)	• Provides a recommendation of research authorisation – including access to data and/or health records.	N/A
Metro South Human Research Ethics Committee (MSHREC)	• When approving a waiver of consent to access data, assess the justification provided by the research team against criteria identified in Section 2.3.10 of the National Statement.	N/A
Data custodian	• Acts as the main point of contact for enquiries regarding confidentiality, privacy and the release of information for their portfolio.	N/A
Health Information Management Services (HIMS) - the 'Data Custodian' for MSH	• Provides support and advice to both the public and staff on how to access medical records held by MSH. • Manages the requests for information received from patients and third parties in accordance with the relevant legislation (including *Hospital and Health Boards Act 2011 (Qld), Right to Information Act 2009 (Qld), Information Privacy Act 2009 (Qld)* and QH Policies). • Manages the requests for medical records for patients, agents representing patients, insurance companies, WorkCover, health professionals, the coroner, Queensland Police Service, courts and other third parties. • Manages all privacy complaints under the position of the Privacy and Confidentiality Contact Officer (PCCO). • Provides training to staff in relation to the release of information, privacy, and confidentiality guidelines.	N/A
Principal Investigator (PI)/ Coordinating Principal Investigator (CPI) - responsible officer	• Be aware of research activities being conducted in their teams. • Maintain local work practices to ensure all researchers are authorised before health records or data is provided.	N/A

Employees, researchers, research student supervisors and students	• Ensure research activities are not conducted without appropriate approval and that participation in research activities only occur where research has been authorised. • Responsible for ensuring appropriate security for any confidential material including that held in computing systems. Where computing systems are accessible through networks, attention to security of confidential data is required. • Responsible for keeping full, accurate and legible records of research methods, research data and primary materials (including laboratory notebooks and electronic data) in a durable, organised, and accessible manner. • Adequate records of the source of research material, experimental data and authorship must be maintained in a secure place after publication and must be recoverable should questions arise.	N/A

DEFINITIONS

Term	Definition
Data	Data refers to research data provided by the Department of Health, an alternative source, or as collected by the researchers themselves.
Data collection methods	Data collection methods in research refer to the systematic approaches and techniques used to gather information for a study. These methods can include surveys, interviews, observations, experiments, and the analysis of existing records or documents. The choice of data collection method depends on the research questions, objectives, and the nature of the study.
Data linkage	Data linkage in research refers to the process of connecting or combining information from multiple sources to create a comprehensive and integrated dataset. This allows researchers to analyse and draw insights from diverse sets of data while maintaining privacy and confidentiality. Data linkage can involve linking data from different sources, such as surveys, administrative records, or databases, to enhance the depth and breadth of research findings.
Data management	A plan that outlines how research data will be handled throughout the entire research lifecycle. It typically includes details on data collection, organisation, storage, sharing, and preservation, ensuring adherence to ethical standards, legal requirements, and institutional policies. A data management plan serves as a roadmap for researchers to manage and safeguard their data effectively.

Confidentiality	In a healthcare setting, confidential information typically refers to sensitive and private data about patients, including their medical records, treatment plans, and any other personal information related to their health. The confidentiality of this information is crucial to maintaining trust between healthcare providers and patients.
Privacy	Privacy in research refers to the protection of individuals' personal information and the assurance that their identities and sensitive data are kept confidential. It involves ethical and legal considerations to safeguard participants from unwarranted disclosure or misuse of their private information during the research process.

RELATED AND SUPPORTING DOCUMENTS

Legislation and other Authority	**Legislation (as updated and replaced from time to time)** • *Hospital and Health Boards Act 2011* (Qld) • *Human Rights Act 2019 (Q*ld) • *Information Privacy Act 2009* (Qld) • *Privacy Act 1988* (Cth) • *Public Health Act 2005* (Qld) • *Therapeutic Goods Act 1989* (Cth) **Regulations** • *Information Privacy Regulation 2009* (Qld) • *Hospital and Health Boards Regulation 2012* (Qld) • *Public Health Regulation 2018* (Qld) • *Therapeutic Goods (Medical Devices) Regulations 2002* (Cth) • *Therapeutic Goods Regulations 1990* (Cth) **Other authority** • Australian Code of the Responsible Conduct of Research (2018) ○ Management of data and information in research guide • National Statement on Ethical Conduct in Human Research (2023) ('National Statement') • Integrated Addendum to ICH E6(R1): Guideline for Good Clinical Practice ICH E6(R2) (2016) **Department of Health** • Health Service Directive: Research Ethics and Governance Directive QH-HSD-035:2023 • Research Management Guideline: external funding and infrastructure support QH-GDL-013-1:2022 • Research Management Policy QH-POL-013:2022

	• Research Management Standard QH-IMP-013:1:2022 • Retention and Disposal of Clinical Records Standard QH-IMP-280-1:2014 • Queensland Health Digital Standard Use of email standard QH-IMP-484-3: 2021 **Metro South Health** • Metro South Health Research Strategy • Finance Management Practice Manual (FMPM) • Human Resources (HR) Delegations Matrix and Schedule • Metro South Financial Delegation Schedule and Framework

Standards	• National Clinical Trials Governance Framework
	• National Safety and Quality Health Service (NSQHS) Standards 2nd Ed.
	  ○ Standard 1 – Clinical Governance
	  ○ Standard 2 – Partnering with Consumers

Supporting documents	**Procedures** • PR2023-411 Research excellence • PR2023-412 Research support and management • PR2023-413 Research administration and compliance **Work instructions** • WI2023-287 Research integrity • WI2023-288 Research quality management systems • WI2023-290 Research authorship, peer review and publication • WI2023-291 Research complaints and misconduct • WI2023-292 Assessing and managing risk in research **Guidelines** • GL2021-75 Partnering with consumers in research • GL2023-97 Aboriginal and Torres Strait Islander health research • GL2023-98 Research translation and impact **Attachments** • Attachment 1: Research project data risk assessment and management plan

HUMAN RIGHTS ACT 2019

Metro South Hospital and Health Service is committed to respecting, protecting and promoting human rights. Under the *Human Rights Act 2019*, Metro South Health has an obligation to act and make decisions in a way that is compatible with human rights and, when deciding, to give proper consideration to human rights. When deciding about research, decision-makers must comply with that obligation. Further information about the *Human Rights Act 2019* is available at: https://www.forgov.qld.gov.au/humanrights.

WORK INSTRUCTION DETAILS

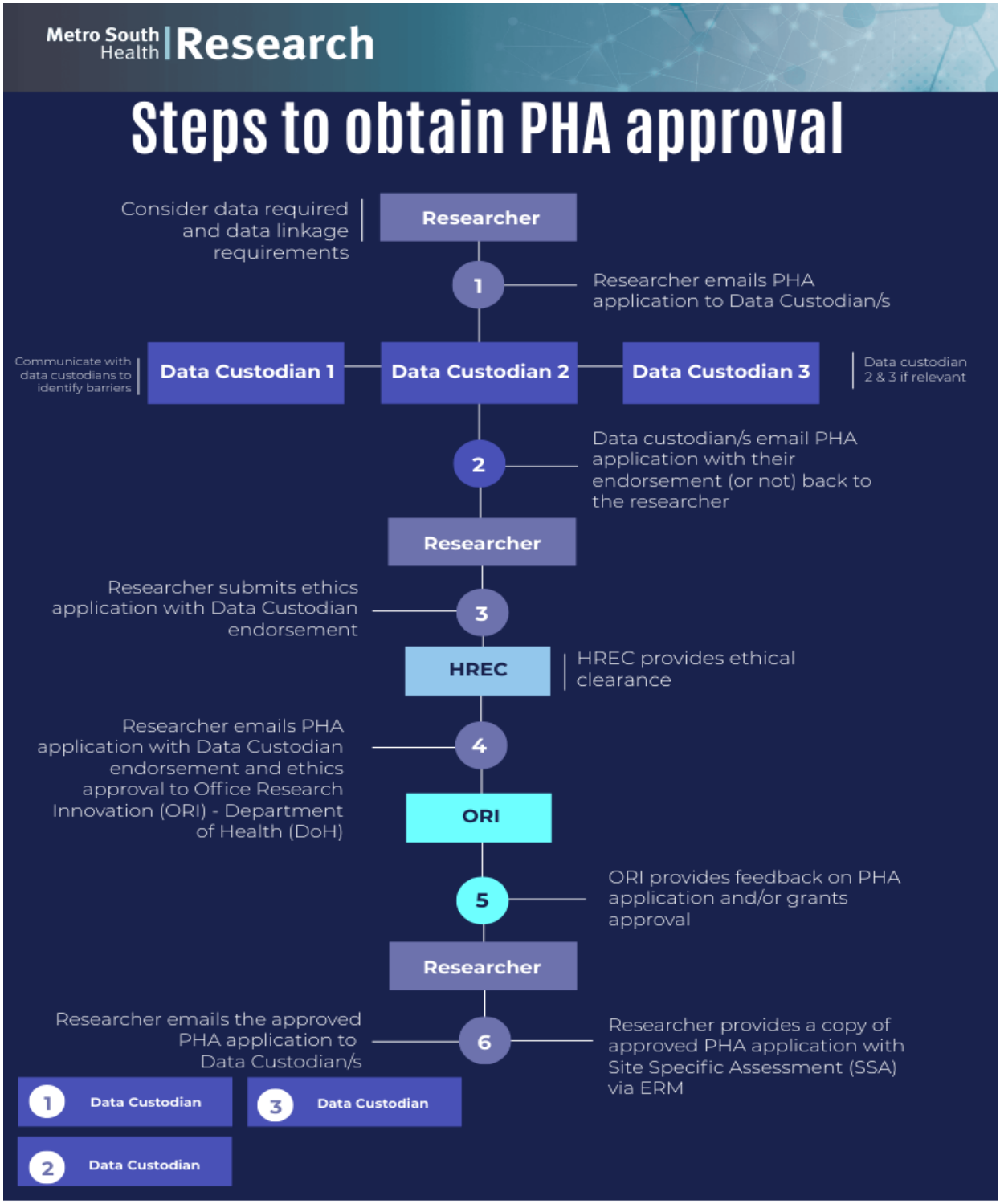
Work Instruction Name	Research data and privacy
Work Instruction Number	WI2023-289
Current Version	V1.2
Keywords	Research data, privacy, information
Aligning MSH or Directorate Procedure Reference	PR2023-411 Research Excellence Procedure
Executive Sponsor	Chief People, Engagement and Research Officer
Document Author	Manager, Research Development, Metro South Research
Next Review Date	December 2026

REVIEW HISTORY

Version	Approval date	Effective from	Executive Sponsor	Comment
1.0	7/12/2023	20/12/2023	Chief People, Engagement and Research Officer	• Supersedes PR2017-125 Research Data Management Procedure
1.1	30/05/2024	03/06/2024	Chief People, Engagement and Research Officer	• Minor update to 5.2 Reporting a privacy breach
1.2	19/08/2024	23/08/2024	Chief People, Engagement and Research Officer	• Minor update to ensure all MSH privacy breaches are reported to the relevant institution's RTI privacy officers • Updated work instruction template.

APPENDICES

1. APPENDIX 1: PHA APPLICATION PROCESS



We care about you

Queensland Government