Mid North Coast Local Health District

Fact sheet

Information for Researchers – Preventing and reporting research-related data or privacy breaches

July 2026

Overview and Scope

This fact sheet applies to all research and ethics-exempt quality projects conducted within MNCLHD.

A data or privacy breach occurs when personal information is accessed, disclosed, lost or used without authorisation. Examples of breaches include:

- Loss or theft of a laptop, USB, mobile device or paper records containing personal information.
- Access to research data by a person who is not authorised to view it.
- Release of information outside the approved dataset.
- Sending identifiable information to the wrong person or email distribution list.
- Publishing or reporting information that could reasonably identify an individual.

Preventing Data and Privacy Breaches

Role of MNCLHD staff or data custodians providing data

Before providing data:

- Confirm the project has the required approval (e.g. HREC approval, site authorisation or ethics exemption).
- Provide only the data approved for the project.
- Check that the dataset matches the approved request and contains no additional information.
- Transfer data only via approved secure methods (e.g. Kiteworks).

Role of Research team in requesting and protecting data

The Research team are responsible for ensuring data is requested, used, stored and shared in accordance with approvals.

When requesting and using data

- Provide clear instructions outlining the approved dataset required.
- Review all data received before use to ensure it matches the approved dataset.
- Use the minimum information necessary for the project.
- Minimise the use of direct identifiers wherever possible (e.g. use age instead of date of birth).

Secure storage requirements

Store data only in approved locations, for example:

- A password-protected file on the NSW Health network.
- A project-specific Teams site accessible only to approved research team members and labelled “Sensitive”.
- NSW Health REDCap with access restricted to approved users and permissions assigned according to role.

- A locked cabinet accessible only to approved research team members.

Do not store research data on USB drives or other portable storage devices.

Access and confidentiality

- Ensure only approved research team members can access the data.
- Ensure all team members understand and comply with project approvals and confidentiality requirements.
- Sign and return confidentiality undertaking (as required).
- Use data only for the approved purpose.

If a suspected or actual breach occurs

Role of Research team in reporting a breach

All members of the research team must report suspected or actual breaches and take immediate action to contain them.

Step 1: Contain the breach

Immediately take steps to prevent further unauthorised access, use or disclosure. Examples include:

- Recovering information that has been accessed, disclosed or lost.
- Restricting access to affected files, systems or folders.
- Changing passwords or access permissions.
- Suspending research activities associated with the breach.

Step 2: Notify the Principal Investigator

Report the breach to the CPI/PI as soon as possible and provide all relevant details.

Step 3: Cooperate with the investigation

Assist with any investigation and implement any actions required to prevent a recurrence.

The role of the Coordinating Principal Investigator and/or Principal Investigator

Step 1: Complete a Data Breach Notification Form and submit it to:

- MNCLHD-RGO@health.nsw.gov.au (research projects), or
- MNCLHD-Research@health.nsw.gov.au (ethics-exempt quality projects).

Step 2: Advise their line manager of:

- the breach;
- actions taken to contain it; and
- actions taken to prevent recurrence.

Step 3: Notify the relevant Human Research Ethics Committee (HREC), via email.

What happens after a breach is reported?

Research Projects

Research Governance Officer (RGO)

- Reviews the breach notification.
- Notifies the District Research Operations Manager (DROM) within 24 hours.
- Completes the Data Breach Self-Assessment Tool within 30 days of becoming aware of the breach.
- Seeks advice from the Data Breach Assessment Officer.
- Advises the research team of the outcome and any required actions.

District Research Operations Manager (DROM)

- Notifies the Director, Research & Knowledge Translation (DRKT).

Ethics-Exempt Quality Projects

District Research Operations Manager (DROM)

- Reviews the breach notification.
- Notifies the Director, Research & Knowledge Translation (DRKT) within 24 hours.
- Completes the Data Breach Self-Assessment Tool within 30 days of becoming aware of the breach.
- Seeks advice from the Data Breach Assessment Officer.
- Advises the project team of the outcome and any required actions.

Data Breach Assessment Officer

- Reviews the assessment.
- Determines whether the breach may be reportable under NSW mandatory notification requirements.
- Register all potential data breaches into the data breach register

Director, Research & Knowledge Translation (DRKT)

- Reviews the recommendation.
- Submits the determination to the Chief Executive (CE) for approval where required.

Further information and Resources

- NSW Health Policy Directive – Data Breaches involving personal or health information (PD2023_040)
- NSW Health Data Governance Framework (GL2019_002)
- NSW Health Policy Directive – Electronic Information Security (PD2026_001)
- Privacy and Personal Information Protection Act 1998
- Health and Records Information Privacy Act 2002

Contact us
For more information, please contact Research & Knowledge Translation Directorate: **E:** MNCLHD-RGO@health.nsw.gov.au or MNCLHD-Research@health.nsw.gov.au