Policy

Effective from: July 2025
Review date: July 2028

Data Breach 010358

NSQHS STANDARDS 1. Clinical Governance

Policy statement

Metro North Hospital and Health Service (Metro North Health) is committed to respecting the privacy and ensuring the security, accuracy and integrity of personal information regarding all patients, staff, contractors and visitors associated with receiving or providing health services. Metro North Health complies with the Queensland Privacy Principles set out in the *Information Privacy Act 2009* (Qld) (IP Act). How Metro North Health manages personal information is detailed in our QPP Privacy Policy and Privacy Plan.

Purpose and intent

The IP Act regulates how Queensland government agencies, such as Metro North Health must comply with the requirements of the Mandatory Notification Data Breach Scheme (MNDB Scheme), effective from 1 July 2025.

This policy:

- identifies the concepts of data breach and eligible data breach
- identifies the obligations under the MNDB Scheme
- outline the principles for reporting and responding to a data breach including a suspected eligible data breach.

Under the MNDB Scheme, the IP Act requires Metro North Health to notify the Queensland Information Commissioner and individuals of data breaches involving personal information (unless an exemption applies) where it is likely that the data breach will result in serious harm.

The *Human Rights Act 2019* (Qld) requires proper consideration to be given to human rights where Metro North Health is contemplating a decision that may affect or limit a human right. This Data Breach Policy together with the Data Breach Procedure supports compliance with the Human Rights Act by facilitating the proper handling and security of personal information and in this way contributing to protection of human rights, including privacy and reputation.

Scope and target audience

This policy applies to:

1. all Metro North Health clinical and non-clinical staff (permanent, temporary and casual) and all organisations and individuals acting as its agents (including Visiting Medical Officers and other partners, contractors, consultants and volunteers)
2. all settings across the health continuum including community, primary, acute, rehabilitation and residential care health services within Metro North Health.

Principles

Metro North Health implements a range of strategies and controls to ensure the security of the personal information it collects, uses and discloses.

All staff have a responsibility to report confirmed or suspected data breaches regardless of whether they meet the criteria of an eligible data breach.

A data breach by a third-party provider may be subject to the MNDB Scheme based on whether Metro North Health has a legal basis that it 'held or holds' the personal information or whether the information is 'under the control' of Metro North Health.

Metro North Health recognises the benefits that responding to and reporting of suspected or confirmed data breaches provide to the organisation both in preventing further data breaches as well as providing opportunities for the individuals affected by a data breach to take steps to protect their personal circumstances.

Metro North Health will take all reasonable steps to contain and minimise the harm that may result as a consequence of a data breach.

Data Breach

A data breach means unauthorised access to, or unauthorised disclosure of information, or loss of information in circumstances where unauthorised access or unauthorised disclosure is likely to occur. A data breach in general includes ALL types of information.

All data breaches must be notified and assessed individually as it is only through investigation is it determined whether the data breach includes personal information. If the data breach includes personal information and is likely to result in serious harm to an individual it will be an 'eligible data breach' and will therefore fall within the notification requirements of the MNDB Scheme. It is also important to note that some data breaches may need to be reported to external agencies such as the Australian Signals Directorate regardless of whether personal information was affected.

A data breach may be caused by malicious action (by an external or internal party), human error or a systemic information handling or information security breakdown.

Some examples of data breaches:

- phishing emails which trick a user into performing an action or providing information
- an email is sent to the wrong recipient
- a file is left in a public place
- lost or stolen laptops, removeable storage devices, or physical files containing personal information
- a staff member accessing a patient record without having a valid work reason for doing so.

Eligible Data Breach

The MNDB Scheme will apply where a suspected or confirmed 'eligible data breach' has occurred.

An eligible data breach is one in which both of the following apply:

- the data breach involves unauthorised access to, unauthorised disclosure of, or loss of personal information held by Metro North Health; and
- the unauthorised access or disclosure is likely to result in serious harm to an individual.

Personal information is defined by s 12 of the IP Act as

> *…information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion—*
>
> *(a) whether the information or opinion is true or not; and*
>
> *(b) whether the information or opinion is recorded in a material form or not.*

The harm that potentially arises from a data breach will vary depending on the nature of the personal information and the context of the data breach.

Serious harm is defined as including:

- serious physical, psychological, emotional, or financial harm to the individual because of the access or disclosure or
- serious harm to the individual's reputation because of the access or disclosure.

The requirement for the risk of serious harm to an individual must be more than a mere possibility, it must be more probable than not. It is not necessary to identify specific individuals who may be harmed, to determine that serious harm is likely to occur for one or more individuals. This is an objective test to be determined based on the facts of a specific breach.

Some of the factors Metro North Health will use in determining serious harm and whether it is likely to result from the data breach may include:

- the kind of personal information accessed, disclosed or lost
- the sensitivity of the personal information
- whether the personal information is protected by one or more security measures
- if the personal information is protected by one or more security measures, the likelihood that any of those security measures could be overcome
- the persons, or the kinds of persons, who have obtained, or who could obtain, the personal information
- the nature of the harm likely to result from the data breach, and
- any other relevant matter.

A data breach may occur within Metro North Health, with other health or government agencies, or where other external persons or entities access data without proper authorisation. A data breach may be due to human error, system or process errors or deliberate acts to access personal information.

Responding to a Data Breach

Metro North Health will undertake a systemic approach to managing a data breach. At all times the underlying principle of *contain and mitigate* will apply in order to minimise any risk of harm that may result from the data breach.

A data breach may be identified by:

- a cyber security breach through monitoring activities
- a staff member identifying an incident
- a staff member identifying a suspected breach through auditing activities

- a member of the public making a complaint about how Metro North Health has managed personal information.

All staff who receive notification of a suspected data breach are responsible for reporting it to the local facility Privacy and Confidentiality Contact Officer (PCCO) or the Director Health Information Policy Access and Coordination (DHIPAC). This may be reported through:

- your line manager/supervisor
- by emailing the details to PrivacyMetroNorth@health.qld.gov.au.

Contain and mitigate

All reasonable steps will be taken to contain the data breach. This obligation to contain and mitigate any harm arising from the data breach is ongoing. The containment measures will depend on the nature of the data breach and may include:

- making efforts to recover the personal information
- securing, restricting access to, or shutting down breached systems in consultation with Digital Metro North
- suspending the activity that led to the data breach
- revoking or changing access codes or passwords.

All reasonable steps will be taken to contain the breach and take appropriate actions to reduce the risk of serious harm for affected individuals.

Assessment

Once the data breach has been contained and the impacts of the data breach have been mitigated, the DHIPAC will determine whether the Data Breach Response Team will be activated to manage the breach. Some of the factors that may lead to the Data Breach Response Team being activated include (but are not limited to):

- the number of individuals affected by the breach
- the breach includes multiple services
- the breach requires input from specialty advisors
- the breach may cause significant harm to individuals affected by the breach
- the breach has been reported in the media.

The members involved in a particular breach will be dependent on the nature of the breach and relevance to the specialty advisor. For example, a data breach involving a paper record will not normally require expertise from the cybersecurity advisor.

Where the Data Breach Response Team is not activated, the data breach will continue to be assessed by the local PCCO and/or DHIPAC in consultation with the relevant service involved in the data breach. Some of the factors that may be considered when assessing a data breach include (but are not limited to):

- the types of information involved in the breach
- the sensitivity of the personal information involved in the breach
- whether the personal information is protected by one or more security measures
- if the personal information is protected by one or more security measures, the likelihood of these measures being overcome
- the kinds of person/s who have or could obtain the personal information

- the nature of the harm likely to result from the data breach
- any other relevant matter.

As soon as practicable but not later than 30 days of becoming aware of a data breach, a decision on whether it is an eligible data breach will be made. Where it is not possible to conclude that the data breach meets the threshold of an eligible data breach within the first 30 days, an extension of time which is reasonably required may be approved by the DHIPAC to complete the assessment.

If an extension is approved, the DHIPAC must give written notice to the Information Commissioner as soon as practicable but no later than the first 30 days.

If the data breach involves a cybersecurity incident Digital Metro North and/or the Queensland Government Information Security Virtual Response Team (QGISVRT) may provide expert assistance in containing and assessing the data that may have been affected by the data breach.

Each data breach will be assessed on an individual basis.

Once the data breach has been contained and assessed, appropriate action will be taken to identify and eliminate the root cause of the data breach. Depending on the cause of the data breach and the steps put in place to contain the data breach, further steps may be required to return to normal operation.

Notification

The DHIPAC must notify the Information Commissioner as soon as practicable after forming the belief the data breach is an eligible data breach. For any data breach that does not meet the criteria as an eligible data breach, consideration will be given to voluntarily reporting the data breach to the Information Commissioner.

Unless an exemption applies, the PCCO and/or DHIPAC, in consultation with relevant business units, will take reasonable steps to facilitate notification to:

- each individual whose personal information was impacted by the eligible data breach, or
- each affected individual, or
- issue a public statement of the eligible data breach if notification to individuals is not reasonably practicable.

The method of communication with individuals will be determined on a case-by-case basis and may include communication through email, telephone or post.

The PCCO and/or DHIPAC will determine whether notification to other agencies or third parties is necessary. Depending on the nature of the eligible data breach, this may include the police, insurance providers, or other State or Commonwealth government agencies.

The PCCO and/or DHIPAC will develop an eligible data breach communications strategy to identify the roles and accountabilities of specific positions in the event of an eligible data breach. This strategy will outline the responsibilities for communications, establish the expected timeframes for notification and a template for communications to notify required individuals.

Where an eligible data breach involves the personal information of children, consideration will be given to the age of the child and whether it is appropriate to provide notification directly to the child or to their parent or guardian. In many cases, if the child is 16 years or over it may be appropriate to provide notification directly to the child. Metro North Health may consult with the relevant treating team for a child before a decision is made.

There is no requirement to notify individuals whose personal information was not involved in the eligible data breach. However, if in the circumstances of the data breach, an individual is identified who is likely to suffer harm for other reasons, Metro North Health may consider notifying these individuals if it is possible to do so without the risk of further breaches. This may form part of the strategy for mitigating any harm from the data breach.

Post-breach review and evaluation

Following the management of an eligible data breach, a post breach review and evaluation may occur to consider any lessons learnt from either the breach itself or the process for managing the data breach.

The complexity of the post-breach review and evaluation process will depend on the severity of the eligible data breach that was investigated. An eligible data breach that required the activation of the Data Breach Response Team should include all team members consulted as well as other staff members who were involved in the response.

Recordkeeping

Any eligible data breach that is not notified directly to affected individuals and does not fall within an exemption, will be published to the Metro North Health website at https://metronorth.health.qld.gov.au/about-us/information-access-privacy.

Metro North Health maintains an internal register of data breaches, including eligible data breaches, which is managed by the DHIPAC.

A number of documents may need to be prepared in responding to a data breach or providing notification under the MNDB Scheme. These documents will be stored securely as required under the *Public Records Act 2023*.

Preventative measures

Metro North Health has the following measures in place to prepare for a data breach.

- A data governance framework encompassing policies and procedures such as Queensland Privacy Principles (QPP) Privacy Policy and Queensland Privacy Principles (QPP) Privacy Plan, Corporate Records Management Policy, Clinical Records Management Policy, Information Security Policy.
- Mandatory Cyber Security Essentials training to assist staff in preventing cyber incidents and avoiding security breaches.
- An Information Security Management System (ISMS based on ISO 27001) program of work
- Privacy awareness training on collection, use and disclosure of personal information.
- Where Metro North Health contracts with external service providers, appropriate privacy obligations will be included in any contracts which outline the information provided, a data breach response plan including timeframes for reporting suspected breaches and provisions around the disposal of data upon termination of the contract.

Mandatory requirements

Where an eligible data breach is reasonably suspected or confirmed, notification must be provided to the Information Commissioner.

Roles and Key Responsibilities

ROLE	ACCOUNTABILITIES
All staff, contractors, volunteers or students	Recognising a data breach incident and reporting it to the line manager or supervisor. Where a data breach incident is notified to the staff member, contractor, volunteer or student, ensuring that the manager or supervisor is notified immediately.

	Take reasonable steps to contain the data breach. Only collecting or creating information required to provide the service. Only retaining information for the length of time that is necessary for the purpose (subject to the *Public Records Act 2023*). Restricting access (physical or electronic) to information only to those authorised to access it.
Managers, supervisors	Ensuring staff under their supervision undergo the mandatory training relating to cybersecurity and privacy, and that staff are aware of the Information Security Policy, Queensland Privacy Principles (QPP) Privacy Policy, this Data Breach Policy and related procedures. Take reasonable steps to contain the data breach. Prompt reporting of any data breaches, suspected data breaches, policy violations reported to the PCCO and/or DHIPAC.
Privacy and Confidentiality Contact Officer (PCCO)	Take reasonable steps to contain the data breach. Assess data breaches that involve personal information at the local facility. Support compliance with record keeping obligations and investigation of complaints and data breaches at the local level. Provide guidance and training to staff on best practice for data breaches at the local facility.
Director Health Information Policy Access and Coordination (DHIPAC)	Take reasonable steps to contain the data breach. Assess data breaches that involve personal information within Metro North Health. Convene the Data Breach Response Team. Coordinate the notification of an eligible data breach to the Information Commissioner and affected individuals. Ensure compliance with record keeping obligations. Coordinate with the Metro North Health leadership team, Digital Metro North, Metro North Legal Services and other key stakeholders in the management of data breaches Develop a communication approach for each data breach. Provide guidance, advice and training to staff on best practice for data breaches.
Metro North Legal Services	Provide legal advice on mandatory notification obligations and other legal questions arising from the management of data breaches under the IP Act as requested by the DHIPAC.
Chief Information Officer	Ensure Digital Metro North validate and rate cyber security incidents, including data breaches, as they occur. Notify the DHIPAC where a cyber incident may involve personal information. Consider whether to notify cyber security agencies where appropriate. Perform the appropriate and necessary containment measures and root cause eradication where the data breach is a system related breach.

	Provide guidance and training to staff on best practice for cyber security.
Executive Director of relevant facility or division	Provide management and decision making for significant eligible data breaches within their area of responsibility.
Metro North Chief Executive	Receive notifications of significant data breaches. Provide management and decision making for significant data breaches across Metro North.

Partnering with consumers

At all times, staff are to act and make decisions in a way that is compatible with human rights by properly considering the human rights of individuals who may be impacted by their actions or decisions in accordance with the *Human Rights Act 2019* (Qld). Partnering with consumers demonstrates respect, integrity and compassion and Metro North Health's commitment to putting values in action, putting people first and providing high quality healthcare outcomes to patients.

Consumers can be referred to the PCCO for the relevant facility or the DHIPAC when a member of the public wishes to make a privacy complaint or have concerns in relation to a potential data breach. For each data breach notified to consumers either through direct notification or publication, an appropriate contact officer will be provided for individuals to make further enquiries of the agency.

Aboriginal and Torres Strait Islander considerations

Metro North Health is committed to protect the public from harm and to improve the quality of health service provision. The National Safety and Quality Health Service (NSQHS) Standards identify six actions specific to the provision care for Aboriginal and Torres Strait Islander people. The attendance to these actions provides assurance that service provision is equitable, and that the needs drive the level and range of care that can be accessed.

See the Australian Commission on Safety and Quality in Health Care for further information

Metro North Health is committed to ensuring our staff have the knowledge and skills to deliver care in culturally capable ways and that our work environments are at all times culturally respectful and supportive of our Aboriginal and Torres Strait Islander staff as guided by the Queensland Health Aboriginal and Torres Strait Islander Cultural Capability Framework 2010-2033 and Metro North Health Equity Strategy 2022-2025.

Culturally and Linguistically Diverse (CALD) patients

Staff are to provide care that encompasses physical, social, emotional, spiritual and cultural wellbeing of the individual, in accordance with the Metro North Collaborating in Health Strategy 2022 – 2024.

The Australian Charter of Healthcare Rights states that patients have a right to be informed about services, treatment, options and costs in a clear and open way. Wherever practical, healthcare providers should take steps to meet patient/consumer access, treatment, language and communication needs.

The principles of equity and cultural safety provide the guiding principles for implementing and maintaining health equity for our diverse communities, including CALD communities, people from refugee and asylum-seeking backgrounds, LGBTQI+ communities, people living with disabilities, rural and remote communities, people who are homeless or vulnerably housed who access health services. These principles are as follows:

Access

Individuals and groups within the organisation will take responsibility for providing a range of access options to health services that are culturally appropriate for CALD patients.

Safety

Patients and other individuals receive safe and high-quality health services, provided with professional care, skill and competence in an environment that makes them feel safe.

Respect

All individuals and groups are treated according to their unique cultural needs and differences with an understanding to not in any way diminish, demean or disempower individuals on the basis of perceived or actual differences.

Partnership

Individuals make decisions with their healthcare provider and are involved in honest and open communication, which includes choosing the people involved in planning and decision-making.

Information

Information is shared with Individuals and groups within the organisation, demonstrating service models that encompass health promotion, disease prevention, diagnostic, treatment, primary, acute, sub-acute and support services.

Privacy

Individuals' privacy will be respected, and their health information will be secure and confidential

Feedback

Individuals share experiences and participate to improve the quality of care and health services. Feedback or complaints will be provided and actioned without effecting the individual's treatment plan. Concerns will be addressed in a transparent and timely way.

Metro North respects, protects and promotes the cultural rights of Culturally and Linguistically Diverse (CALD) people. Please advise CALD patients, their families and/or substitute decision-makers of their cultural and language rights under Section 27 of the *Human Rights Act* (2019). An interpreter may be booked to promote consumers' cultural right to communicate in a language of their choosing on the Metro North Intranet Language Services page.

Legislation and other authority

Public Sector Ethics Act 1994 (Qld)

Information Privacy Act 2009 (Qld)

Right to Information Act 2009 (Qld)

Hospital and Health Boards Act 2011 (Qld)

Human Rights Act 2019 (Qld)

Public Health Act 2005 (Qld)

Public Records Act 2023 (Qld)

Human Rights

This policy has been reviewed in line with the *Human Rights Act 2019* (Qld) and no human rights have been limited by the processes outlined in this document. More generally, the policy should help achieve a positive outcome for the human right of privacy.

Related Documents

Metro North Health Queensland Privacy Principles (QPP) Privacy Policy

Metro North Health Queensland Privacy Principles (QPP) Privacy Plan

Metro North Health Procedure 004221 CCTV/Body Worn Cameras/Photographs and Filming

Metro North Health Procedure 004223 Administrative Access to Health Records

Metro North Health Procedure 004547 Queensland Privacy Principles (QPP) Privacy

Metro North Health Procedure 006677 Data Breach

Metro North Health Procedure 005458 Information Access – Access and Amendment under Right to Information

Metro North Health How to Handle Privacy Complaints Guide

Appendix 1 – Definition of terms (if required)

Term	Definition	Source
data breach	… either of the following in relation to information held by the agency— (a) unauthorised access to, or unauthorised disclosure of, the information; (b) the loss of the information in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur.	Information Privacy Act 2009 (Qld) Sch 5
data breach response team	Specific units or positions that have been identified as critical to managing a data breach including those identified as an eligible data breach. The composition of the team will vary depending on the type of information involved, the severity of the breach and the steps required in order to mitigate any resultant harm.	
eligible data breach	An eligible data breach of an agency is a data breach of the agency that occurs in relation to personal information held by the agency if— (a) both of the following apply— (i) the data breach involves unauthorised access to, or unauthorised disclosure of, the personal information; (ii) the access or disclosure is likely to result in serious harm to an individual (an affected individual) to whom the personal information relates, having regard to the matters stated in subsection (2); or (b) the data breach involves the personal information being lost in circumstances where— (i) unauthorised access to, or unauthorised disclosure of, the personal information is likely to occur; and (ii) if the unauthorised access to or unauthorised disclosure of the personal information were to occur, it would be likely to result in serious harm to an individual (also an affected individual) to	Information Privacy Act 2009 (Qld) s 47

	whom the personal information relates, having regard to the matters stated in subsection (2).	
exemption to notification	The following circumstances may result in an individual not being notified of the eligible data breach: • complying with the notification obligation is likely to prejudice an investigation that could lead to the prosecution of an offence or proceedings before a court or tribunal • the eligible data breach involves more than one agency, and another agency is undertaking the notification obligations • action has been taken to mitigate the unauthorised access, disclosure or loss and as a result of that action the data breach is no longer considered likely to result in serious harm to any individual • complying with the notification obligation is inconsistent with a provision of an Act of the Commonwealth or a State that prohibits or regulates the use or disclosure of the information • complying with the notification obligation would create a serious risk of harm to an individual's health or safety • complying with the notification obligation is likely to compromise or worsen the agency's cybersecurity or lead to further data breaches.	Information Privacy Act 2009, ch 3A, pt 3, div 3.
information management	The means by which an organisation plans, identifies, creates, receives, collects, organises, governs, secures, uses, controls, disseminates, exchanges, maintains, preserves and disposes of its information as well as any means through which the organisation ensures that the value of that information is identified and exploited to its fullest extent.	Metro North Health Information Management Principles
likely to result	…more than merely possible; more probable than not to occur. Factors to consider: (a) the kind of personal information accessed, disclosed or lost; and (b) the sensitivity of the personal information; and (c) whether the personal information is protected by 1 or more security measures; and (d) if the personal information is protected by 1 or more security measures—the likelihood that any of those security measures could be overcome; and (e) the persons, or the kinds of persons, who have obtained, or who could obtain, the personal information; and (f) the nature of the harm likely to result from the data breach; and (g) any other relevant matter.	Office of the Information Commissioner Guideline, Mandatory Notification of Data Breach Scheme, August 2024, page 7. Information Privacy Act 2009 (Qld) s 47(2)

loss	The information or device was lost in circumstances where there is a risk of unauthorised access or disclosure. For example, a USB device was left on the train, and someone picked up the device.	Office of the Information Commissioner Guideline, Mandatory Notification of Data Breach Scheme, August 2024, page 4-5.
non-eligible data breach	A data breach which does not meet the requirement for notification as an eligible data breach.	Information Privacy Act 2009 (Qld) s 47
personal information	Personal information means information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion— (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not.	Information Privacy Act 2009 (Qld) s 12
privacy complaint	A privacy complaint is a complaint by an individual about an act done or practice engaged in by a relevant entity in relation to the individual's personal information that may be a breach of the relevant entity's obligation to comply with— (a) the privacy principle requirements; or (b) for an agency—chapter 5.	Information Privacy Act 2009 (Qld) s 164
sensitive information	(a) …personal information about the individual that includes any of the following— (i) racial or ethnic origin; (ii) political opinions; (iii) political association; (iv) religious beliefs or affiliations; (v) philosophical beliefs; (vi) professional or trade association; (vii) membership of a trade union; (viii) sexual preferences or practices; (ix) criminal record; or (b) health information about the individual; (c) genetic information about an individual that is not otherwise health information; (d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification or biometric templates.	Information Privacy Act 2009, sch 5
serious harm	**serious harm**, to an individual in relation to the unauthorised access or unauthorised disclosure of the individual's personal information, includes, for example— (a) serious physical, psychological, emotional or financial harm to the individual because of the access or disclosure; or (b) serious harm to the individual's reputation because of the access or disclosure.	Information Privacy Act 2009, sch 5

unauthorised access	The information has been accessed by someone who has not been granted access to the information. For example, a computer system left unattended was accessed by an individual who has not been granted a username for the system.	Office of the Information Commissioner Guideline, Mandatory Notification of Data Breach Scheme, August 2024, pages 3-4.
unauthorised disclosure	This information has been disclosed to an incorrect recipient or where there was no legal basis to disclose the information. For example, a discharge summary for a patient was inserted into an incorrect envelope and sent to another patient.	Office of the Information Commissioner Guideline, Mandatory Notification of Data Breach Scheme, August 2024, page 4.

Document History

Author	Director Health Information Policy Access and Coordination
Custodian	Director Health Information Policy Access and Coordination
Consequence level/ Risk	**Likelihood –** Possible **Consequence –** Minor **Risk Rating –** Medium (9)
Compliance evaluation and audit	Privacy compliance assessed and evaluated at Metro North committees including Metro North Information Access Committee, and Metro North Information Management Committee. Privacy Impact Assessment process has been established and includes review by privacy subject matter experts. The Office of the Information Commissioner (OIC) will be notified of eligible data breaches and an internal register of data breaches will be maintained and reviewed annually. It also has jurisdiction for review of privacy complaints and an auditing function of agency compliance with the legislation.
Replaces Document/s	N/A
Changes to practice from previous version	N/A
Education and training to support implementation	Marketing through regular email to all line managers of new and updated policies and procedures; Also, a notification through Safety and Quality Units to key stakeholders.
Consultation	**Key stakeholders** Information Access Committee **Broad Consultation** facilitated through the following**: (do not delete this list)** Metro North Aboriginal and Torres Strait Islander Leadership Team Metro North Clinical Governance Safety, Quality and Risk Digital Metro North Metro North Medical Services Metro North Nursing and Midwifery Services

	Metro North Allied Health Metro North Communication Metro North Finance Metro North Norfolk Island Support Program Metro North People and Culture Metro North Workplace Health and Safety Metro North Legal Services Metro North Ethical Standards Unit Metro North Risk and Compliance Officer Metro North Clinical Streams Metro North Engage Health Excellence Innovation Unit Clinical Directorate Safety and Quality Units Clinical Skills Development Centre
Marketing Strategy	A Policy, Procedure and Protocol Staff Update will be published online each month to update staff of all new and updated policies, procedures and protocols. This update will be emailed to all Safety and Quality Units in each clinical directorate and a broadcast email sent to all Metro North Health staff with a link to the published update.
Key words	privacy, data breach, eligible data breach, privacy breach, personal, information, management, QPPs, Queensland Privacy Principles, right to information, anonymity, security, policy, metro north, 010358

Custodian Signature Date

Director Health Information Policy Access and Coordination, Metro North Hospital and Health Service

Authorising Officer Signature Date

Chief Finance and Corporate Officer, Metro North Hospital and Health Service

AUTHORISATION

Signature Date

Chief Executive, Metro North Hospital and Health Service

The signed version is kept in file at Clinical Governance, Safety, Quality and Risk, Metro North Health.