

Privacy and confidentiality

Version: 2

Published: 27 Oct 2026, 11:00 AM

Last edited: 27 Oct 2026, 10:57 AM

Approved: 27 Oct 2026, Ryan Wait

Next review: 1 Dec 2027

Introduction

This policy ensures we protect and handle personal information in accordance with the NDIS and relevant privacy legislation. We acknowledge an individual's right to privacy while recognising that personal information is required to be collected, maintained and administered in order to provide a safe working environment and a high standard of quality.

The information we collect is used to provide services to participants in a safe and healthy environment with individual requirements, to meet duty of care obligations, to initiate appropriate referrals, and to conduct business activities to support those services.

Applicability

When

- applies to all personal information and sensitive personal information including the personal information of employees and participants
- applies to all company confidential information - that is any information not publicly available.

Who

- applies to all representatives including key management personnel, directors, full time workers, part time workers, casual workers, contractors and volunteers.

Governing obligations for this policy



NDIS Practice Standards 1.3.1 Privacy and dignity



NDIS Practice Standards 1.3.3 Privacy and dignity



NDIS Practice Standards 3.1.2 Access to supports

Governing regulations for this policy



NDIS (Provider Registration and Practice Standards) Rules 2018 (Cth)



NDIS (Quality Indicators) Guidelines 2018 (Cth)



Privacy Act 1988 (Cth)



Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth)



Privacy and Personal Information Protection Act 1998 (NSW)

Documents relevant to this policy



Privacy and confidentiality guidelines

To protect the privacy and confidentiality of individuals, MMT Care will:

- Use or disclose personal information only for the purpose for which it was collected, with consent, or where otherwise permitted or required by law. Limit information shared to what is reasonably necessary.
- Explain relevant information-sharing arrangements, including with treating professionals, support coordinators, plan managers, technology providers, auditors and government bodies.
- Use de-identified information for reporting where appropriate. Where identifiable information is necessary for claims, regulatory reporting or another lawful purpose, disclose only the information required.
- Provide a clear process for individuals to request access to their personal information or correction of inaccurate, incomplete or outdated information. Explain any lawful refusal and available complaint options.
- Obtain specific informed consent for photographs, audio recordings and video recordings, including their intended purpose and use, unless otherwise authorised by law. Consent for promotional use must be separate from consent relating to support delivery.
- Explain external NDIS audit arrangements and participants' choices about interviews and access to their records, subject to applicable legal requirements.
- Manage any use of personal information in AI tools in accordance with the **Artificial Intelligence (AI) use**, including its approval, consent and human-review requirements.
- Provide accessible information about how to raise a privacy concern or complaint, including the relevant internal contact and external Complaint management pathways.

Security of information

To keep personal and confidential information secure, MMT Care will:

- Take reasonable steps to protect information from misuse, interference, loss, unauthorised access, modification and disclosure.
- Restrict access to authorised personnel who require the information to perform their duties. Review access permissions regularly and promptly update or remove access when responsibilities change or employment ends.
- Use approved systems with appropriate safeguards, including individual user accounts, strong passwords, multi-factor authentication where available, and encryption in transit and at rest where appropriate to the risks.
- Keep paper records, portable devices and other storage media secure, including through locked storage and physical access restrictions.
- Require workers to use approved communication and file-sharing methods, verify recipients before sending information, and avoid personal email accounts or unapproved applications.
- Protect information when working remotely or in the community by securing devices, locking unattended screens and preventing conversations or records from being overheard or viewed by unauthorised people.
- Assess external service providers that store or process information, including cloud and AI providers, for appropriate privacy and security safeguards, access arrangements, storage locations and overseas handling.
- Maintain appropriate backups and recovery arrangements, and keep systems updated to reduce security vulnerabilities.
- Retain information in accordance with applicable legal requirements and MMT Care's records-retention arrangements. Securely destroy or de-identify information when it is no longer required, provided no legal obligation or hold requires its retention.
- Provide workers with training on secure information handling and require immediate reporting of lost devices, misdirected communications, unauthorised access or other suspected security breaches.

These requirements apply to information held in electronic, paper, photographic, audio and video formats and should be read alongside MMT Care's **Artificial Intelligence (AI) use** and relevant records-management and incident-management procedures.

Data breaches

A data breach occurs when personal information is lost or accessed or disclosed without authorisation. This may include misdirected emails, lost records or devices, inappropriate access to participant files, cyberattacks or unauthorised uploads to AI tools.

MMT Care will:

- Require all workers to immediately report actual or suspected data breach to their manager or the designated privacy lead and record them through the incident-management process.
- Take immediate steps to contain the breach, prevent further exposure, preserve relevant evidence and reduce potential harm.
- Assess the information involved, the people affected, the likely consequences and whether remedial action can prevent serious harm.
- Where an eligible data breach is suspected, conduct a reasonable and expeditious assessment, taking all reasonable steps to complete it within **30 calendar days** of becoming aware of the grounds for suspicion.
- Where there are reasonable grounds to believe an eligible data breach has occurred, notify the **Office of the Australian Information Commissioner (OAIC)** and affected individuals as soon as practicable, unless a legal exception applies. Notification must not be delayed until the end of the assessment period.
- Explain notifications in accessible language, including what happened, the types of information involved, recommended protective steps and a contact for assistance.
- Consider any separate reporting obligations to the NDIS Commission or other authorities. A privacy breach does not automatically constitute an NDIS reportable incident.
- Document the assessment, remedial actions, notification decisions and reasons, including where notification is not required.
- Review the incident and implement improvements to systems, procedures and worker training to reduce the likelihood of recurrence.

An **eligible data breach** generally involves unauthorised access, disclosure or loss of personal information that is likely to result in serious harm, where remedial action has not prevented that likely harm.

Breach of privacy and confidentiality

MMT Care will:

- Require workers to immediately report any actual or suspected breach to their manager or the designated privacy lead.
- Take prompt action to protect affected individuals, limit further disclosure and preserve relevant evidence.
- Assess the circumstances and undertake an investigation where appropriate, ensuring procedural fairness and confidentiality.
- Apply the **data breach** requirements where personal information is involved, including assessment and notification obligations where applicable.
- Determine corrective action based on the seriousness of the breach, its impact, whether it was deliberate or accidental, and any contributing system or training issues.
- Take disciplinary action where warranted, up to and including termination of employment, subject to a fair process and applicable employment obligations.
- Implement and document any required improvements to practices, systems, supervision or training.
- Ensure individuals can raise concerns or report suspected breaches in good faith without retaliation or disadvantage.

Confidentiality obligations continue after employment, engagement or service delivery ends. These obligations do not prevent lawful reporting to regulators, police or other authorised bodies, or disclosures protected by law.