PRIVACY
POLICY AND PROCEDURES

CONTENTS

AUTHORISATION

Authorised by: Chief Executive Officer
Date Effective: January 2024
Review/Consultation: Leadership Team
Review Date: January 2026

DISTRIBUTION: Board, Leadership Team and workforce (employees, contractor and volunteers).

RISK: High

POLICY

Harbison Board and Leadership Team will act in a serious and committed manner to meet their obligations under the *Privacy Act 1988* (Cth) ensuring personal and sensitive information is collected, held, used, and disclosed in accordance with the Australian Privacy Principles (APP) and the Aged Care Quality Standards. This includes:

- The obligations under the Australian Privacy Principles (APP), as set out in the *Privacy Act 1988* (Cth) and the *Privacy Amendment (enhancing Privacy Protection) Act 2012* (Cth), *Aged Care Act 1997* and *NDIS Act 2013* and NDIS Practice Standards, will be adhered to.
- All legislated notifiable breaches are identified, investigated and communicated as per legislative requirements of *The Privacy Amendment (Notifiable Data Breaches) Act 2017* and Quality of Care Principles 2014.
- The privacy and confidentiality rights of residents, members of the workforce and visitors to the Home will be respected.
- That residents, the workforce and visitors are informed of, and understand the surveillance mechanisms in place, and the requirements of the *Surveillance Devices Act 2007* in the Home.

PROCESS CHECKLIST

Steps		
One	CEO, CCM, and Workforce responsibilities	☐ To ensure a system in place meeting legislated privacy requirements for all stakeholders ☐ Report any breaches of privacy to their supervisor or the Privacy Officer immediately
Two	Obtain consent	☐ Obtain resident consent on admission
Three	Registry Entry	☐ Enter resident consent in Privacy Register
Four	Collection and Use of Personal Information	☐ Collect only personal, and sensitive information where necessary to provide health services ☐ Destroy unsolicited personal information and information that is no longer required for the delivery of health services
Five	Access and disclosure of personal and sensitive information	☐ Follow policy direction for access and disclosure of personal information and sensitive information
Six	Surveillance	☐ Ensure that optical surveillance devices are used with the consent of resident/Person Responsible or member of the workforce, and surveillance signage is installed on all external doors ☐ No personal devices to be used for surveillance. ☐ Report any matters of concern to the RN in charge or supervisor
Seven	Breaches of Privacy	☐ Follows policy direction for breaches of privacy

KEY DEFINITIONS

Listening device	Any device capable of being used to overhear, record, monitor or listen to a conversation or words spoken to or by any person in conversation, but does not include a hearing aid or similar device used by a person with impaired hearing to overcome the impairment.
Health information	A subset of sensitive information health information, under the Privacy Act 1988, is: • 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. • Other personal information collected to provide, or in providing, a health service to an individual. • Other personal information collected in connection with the donation, or intended donation, by an individual of his or her body parts, organs or body substances. • 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.
Neglect	Subsection 15NA (10) of the Quality-of-Care Principles states that neglect of a resident includes: • A breach of the duty of care owed by the provider, or a workforce member of the provider, to the resident. • A gross breach of professional standards by a workforce member of the provider in providing care. • or services to the resident.
Notifiable data breach	Where there has been unauthorised access or disclosure of personal information it holds, or such information has been lost in circumstances where that's likely to lead to unauthorised access or disclosure; and a reasonable person would conclude that such access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates.
Open disclosure	The open discussion that an aged care provider has with people receiving aged care services when something goes wrong that has harmed or had the potential to cause harm to a person receiving an aged care service.
Optical surveillance device	Any device capable of being used to record visually or observe an activity, but does not include spectacles, contact lenses or a similar device used by a person with impaired sight to overcome that impairment.
Personal information	Any information or an opinion about an identified individual, or an individual who is reasonably identifiable.
Person Responsible	A Person Responsible is not necessarily the resident's next of kin or carer. Under section 33A(4) of the Guardianship Act 1987, there is a hierarchy of people who can be the Person Responsible. A Person Responsible is one of the following people in order of priority.

	1. Guardian – An appointed guardian (or enduring guardian) who has been given the right to consent to medical and dental treatments, or 2. Spouse or partner – If there is no guardian, a spouse, de-facto spouse or partner where there is a close continuing relationship, or 3. Carer – If there is no spouse or partner, an unpaid carer who provides or arranges for domestic support on a regular basis, or 4. Relative or friend – If there is no carer, a friend or relative who has a close personal relationship, frequent personal contact and a personal interest in the person's welfare, on an unpaid basis
Reportable incident (Aged Care Quality and Safety Commission - ACQSC)	Under section 54-3 of the Aged Care Act, (and section 15NA of the Quality-of-Care Principles), a reportable incident is any of the following incidents that have occurred, are alleged to have occurred, or are suspected of having occurred to a residential resident, in connection with the provision of residential care, or flexible care provided in a residential setting that are reportable the Aged Care Quality and Safety Commission: • Unreasonable use of force against a resident. • Unlawful sexual contact, or inappropriate sexual conduct, inflicted on a resident. • Psychological or emotional abuse of a resident. • Unexpected death of a resident. • Stealing from, or financial coercion of, a resident by a member of the workforce (this includes anyone employed, hired, retained, or contracted by the provider). • Neglect of a resident. • Use of physical or chemical restraint of a resident (other than in the circumstances set out in the Quality-of-Care Principles). • Unexplained absence of a resident from the service.
Sensitive information	Is a subset of personal information and is defined as information or an opinion (that is also personal information) about an individual's: • Racial or ethnic origin; political opinions; membership of a political association; religious beliefs or affiliations; philosophical beliefs; membership of a professional or trade association; membership of a trade union; sexual preferences or practices; or criminal record. • Health information about an individual. • Genetic information (that is not otherwise health information). • Biometric information that is to be used for the purpose of automated biometric verification or biometric identification. • Biometric templates.

Serious Incident Response Scheme (ACQSC)	The scheme established to prevent, and reduce the risk of, incidents of abuse and neglect in Australian Government-subsidised residential aged care. It requires providers to have an effective incident management system in place and to identify, record, manage, resolve, and report all serious incidents that occur, or are alleged or suspected to have occurred.
Surveillance device	A data surveillance device, a listening device, an optical surveillance device, or a tracking device.
Safety device (tracking)	Any electronic device capable of being used to determine or monitor the geographical location of a person or an object.
Valid informed consent	Informed consent is achieved through a process of communication, discussion, and shared decision making. It involves understanding the person's goals and concerns, and discussing with the person (or their substitute decision-maker) their options for treatment, the potential outcomes (positive, negative and neutral), risks and benefits and what this might mean for them. The person or their substitute decision-maker will make an informed decision based on this information. Informed consent in health care for there to be valid informed consent, the person consenting must: • Have the legal capacity to consent • Give their consent voluntarily • Give their consent to the specific treatment, procedure or other intervention being discussed • Have enough information about their condition, treatment options, the benefits and risks relevant to them, and alternative options for them to make an informed decision to consent. This includes the opportunity to ask questions and discuss concerns. A person can give consent expressly (in writing or verbally) or it can be implied. Consent by a person must be in writing when required by law or by the policies of the state, territory or healthcare organisation where the person is receiving care and treatment. The most appropriate form of consent will depend on the degree of risk and complexity of the treatment for that person.

PROCEDURES

Responsibilities

- The Chief Executive Officer (CEO) is responsible to ensure there is a system at the Home that meets legislated privacy requirements for all stakeholders. This includes an effective system that manages and safeguards the following in relation to personal information:
    - Information provision and consent
    - Appropriate collection
    - Storage
    - Distribution.
- The CEO and Clinical Care Manager (CCM) must ensure there is a system to safeguard the personal privacy of all residents, including maintaining privacy in the delivery of care and clinical care.
- Where privacy is requested by a resident, Person Responsible, member of the workforce or other stakeholder of Harbison and cannot be maintained due to legislative requirements, the CEO is responsible to ensure there is a timely and system to notify stakeholders of this requirement.
- The workforce is responsible for ensuring the privacy of residents, other workers and visitors is safeguarded in accordance with their training and role responsibilities. This includes the obligation to report any breaches of privacy to their supervisor or the Privacy Officer immediately.

Personal and Sensitive Information

The CEO is responsible for oversighting the collection and safe storage of personal and sensitive information of residents and workforce, where applicable (employees, volunteers and contractors). 'Personal information' means information Harbison holds about you from which your identity is either clear or can be reasonably determined. The personal information Harbison may hold includes the following:

- residents
    - Accident and Incident Forms.
    - Aged Care Assessment Team records entered on the ‘My Aged Care’ system.
    - Care and service plans.
    - Clinical information including assessments and monitoring charts.
    - Commonwealth AN-ACC funding information.
    - resident Agreements.
    - Country of birth and whether Aboriginal and/or Torres Strait Islander origin.
    - Criminal record.

- Current address.
- Date of birth.
- Entitlement details including Medicare, pension and health care fund.
- Family medical history.
- Financial and billing information including Income and Asset Notifications.
- Medical history, including influenza and COVID-19 vaccination status and we may request health information and genetic information that is not otherwise health information (in keeping with the definition under the Privacy Act 1988) as required.
- Medication charts.
- Name.
- NDIS Support Plan and other Plans.
- Next of kin details/Person Responsible.
- Nursing, medical and allied health information.
- Pathology results.
- Person responsible for resident, e.g., Power of Attorney, Enduring Power of Attorney, Guardian, Trustee, etc.
- Photographs (for medical purposes such as medication administration).
- Progress notes.
- Racial/ ethnic origin.
- Religious belief or affiliations.
- Sexual preferences or practices.
- Social history.
- X-ray results.

- Workforce (as applicable to the worker's role):
  - Address and contact details.
  - Bank account details (where applicable for volunteers, e.g., reimbursements).
  - Citizenship, passport and/or visa permit.
  - Employment history.
  - Employment references.
  - HR/personnel records including superannuation fund.
  - Influenza and COVID-19 vaccination records.
  - Name.
  - National Police Certificate (Criminal History Record Check) or NDIS Worker Screen Check, as applicable or Prohibition order (as applicable to the role).
  - Occupation.
  - Qualifications, training, registration status, licence/s and competency records.
  - Workers' compensation or injury information.

- Employees and volunteers. The following is also collected:
  - Application Form.
  - Date of birth/country of birth.
  - Details of next of kin.
  - Medical history or fitness for work information, relevant to role.
  - Racial/ ethnic origin, e.g., languages spoken, to celebrate diversity.
  - Tax file number.
- Contractors. The following is also collected:
  - Contractor Agreement.
  - Insurances including workers' compensation, professional and public liability.

Information Provision and Training

The CEO must ensure:

- Residents and persons responsible receive information relating to privacy rights and responsibilities and consent on admission, during orientation and ongoing via care conference, resident meetings, newsletters and any other means. This includes residents and Person Responsible being informed of their obligation to respect the privacy of others living and working at the Home and the ways they can meet these obligations.
- The workforce receives privacy information and where applicable, training at orientation and ongoing, specifically in respect to:
  - Maintaining legal and regulatory requirements.
  - Protection of any personal records in use at the Home.
  - Maintaining privacy in the delivery of personal care (as applicable to role).
  - Communicating in a way that maintains privacy.
  - Understanding the requirements and principles for informed and valid consent, respectively and applying these in practice, as applicable to role.
- Refer also to Dignity Policy and Procedures: resident personal privacy in the delivery of care.

Consent

The CEO must ensure:

- Resident consent to privacy and sensitive information arrangements is obtained on admission to the Home via the resident Privacy Agreement.
- Resident consent is reviewed every 12 months in line with the annual case conference process. Where the resident is unable to provide written consent but has capacity to consent, the Privacy Agreement will be completed in accordance with the resident's wishes by the RN and a file note will be placed on the form reflecting the

date, record of communication and consent and the name and designation of the person obtaining consent.

- A Privacy and Confidentiality Agreement for workers and volunteers is made upon employment and engagement, respectively.
- A Privacy Register is in operation that records the wishes of residents where they *do not* agree with any of the privacy options on the resident Privacy Agreement. This register must be maintained as current by the Lifestyle Coordinator, with oversight by the Clinical care manager, and must be available to any members of the workforce who are collecting and releasing resident's personal information.
- Where there is a specific request from the resident or Person Responsible to release information to a third party (other than those indicated in the Collection and Use of Personal Information), consent is obtained from the resident or Person Responsible in writing through the completion of a Privacy Consent Form – External Services.
- There is a system and appropriate support for residents to withdraw or alter their privacy consent at any time.

Collection and Use of Personal Information

The CEO will be responsible to ensure:

- In most cases Harbison information is collected directly from the individual with their consent.
- Personal and sensitive information may be gathered from forms, telephone calls, faxes, emails, face to face meetings, interviews and assessments.
- Generally, only personal and sensitive information is collected if it is necessary to provide health services and to comply with our obligations under Australian law (e.g., tax office obligations, immigration legislation, industrial instruments, etc., National Aged Care Mandatory Quality Indicator Program) or a court/tribunal order.
- Where information is collected from other sources, Harbison will inform the individual that Harbison holds their personal information.
- Unsolicited personal information and information that is no longer required for the delivery of health services will be destroyed or de-identified as soon as practicable if it is lawful and reasonable to do so.
- The potential consequences of not allowing us to collect and hold the required personal information are that Harbison may be unable to:
    - Provide appropriate health care and health services and meet our legislated obligations.
    - Meet the individual requirements of the resident.
    - Provide continuing employment to an employee.
    - Continue with the services of a contractor or volunteer.

- If Harbison receives 'unsolicited information' such as personal information that is not relevant to the functions of the organisation, it will 'de-identify or destroy the information as soon as practicable'.

Disclosure of Personal Information

The CEO will be responsible to ensure:

- Personal information may be disclosed if Harbison:
  - Is required or authorised by Australian law or a court/tribunal order.
  - Reasonably believes that the disclosure is necessary to lessen or prevent a serious or imminent threat to an individual's life, health or safety, or a serious threat to public health or safety.
  - Has reason to believe that an unlawful activity has been, is being, or may be engaged in.
- Personal information may be disclosed to other persons as part of the provision of health services, including:
  - Other health care professionals that are or may be involved in the care of residents or employees including general practitioners, hospitals, NDIS support services and other allied health providers
  - Other external agencies that Harbison have contracts to provide services to residents and employees on our behalf. In circumstances where this is necessary, these external agencies are required to provide confirmation of their compliance with the *Privacy Act 1988* (Cth).
  - Funding bodies and other government agencies as required by Commonwealth and State legislation.
  - To the resident or the 'Person Responsible' for giving and accessing their information.
  - To the person(s) paying or guaranteeing payment of your account.
  - As required to any third party including external service providers, collection agencies and legal firms required to obtain payment of your account under this agreement.
  - Legal or government agencies, where required by law e.g., where we receive a subpoena to obtain your records, where a crime has been committed and we are required by law or following a critical incident, i.e., Police.
- If it is necessary to transfer personal information to someone overseas, Harbison will comply with this policy and the APPs and take reasonable steps to ensure that the recipient does not breach the APPs in relation to that information.

- Personal information relating to any group or individual will not be used for other purposes such as fundraising or direct marketing activities without seeking written consent of the person or the 'Person Responsible' for the resident.
- residents, Person Responsible and visitors must also maintain the privacy of other residents living in the home. The Consumer Privacy Agreement specifically outlines this requirement. Signage and workforce protocols in the Home will also reinforce this requirement, e.g., not providing information to a resident or a (visitor) without resident consent.
- De-identified information is used wherever possible.

Disclosure of Sensitive Information

- Sensitive information will only be disclosed in the following circumstances:
    - For the primary purpose it was intended or for a secondary purpose that is directly related to the primary purpose of collection and within the reasonable expectations of the individual, e.g., an auditor may review and report on sensitive information in a resident file where it pertains to providing quality care and services under the Aged Care Quality Standards. The purpose is directly linked to the primary purpose of collecting the information.
- Sensitive information will not be used or disclosed in the following circumstances:
    - For the secondary purpose of direct marketing.
    - To 'related bodies corporate' in the same way that they may share other 'personal information'.

Security of Personal Information

The CEO will be responsible to ensure:

- Harbison takes all reasonable steps to protect the personal information Harbison holds from misuse and loss, and from unauthorised access, modification or disclosure.
- All personal information is held in a secure and confidential manner and reasonable steps are taken to ensure personal information is secure (e.g., all computers have password access, and personal information is kept in secure areas).
- All electronic systems that hold personal information have up to date security protection systems. These are reviewed on a regular basis and tested to ensure they are efficient and able to meet any potential 'interference' that might occur.
- Harbison will ensure secure disposal of electronic and paper-based records.
- In the event of loss of personal information, Harbison will:
    - Seek to identify and secure the breach to prevent further breaches.
    - Assess the nature and severity of the breach.

- Commence an internal investigation in relation to the breach.
- Report the breach to police where criminal activity is suspected.
- Notify the Office of the Australian Information Commissioner if the data breach is likely to cause serious harm under the Notifiable Data Breaches scheme.
- Inform the affected individual(s) where appropriate and possible so that individuals have the opportunity to take steps to protect their personal information after a data breach.

Access to Personal Information

The CEO will be responsible to ensure:

- All reasonable steps are taken to provide access to the personal information that Harbison holds within a reasonable period of time in accordance with the Australian Privacy Principles.
- There is communication to all stakeholders that requests for access to the personal information Harbison holds should be made in writing to the Privacy Officer.
- Harbison does not provide access to the personal information Harbison hold about an individual when:
  - Release of the personal information would be unlawful.
  - The information may be subject to legal proceedings.
  - Release of the personal information would pose a serious threat to the life, health or safety of an individual or to public health or public safety.
  - Release is likely to have an unreasonable impact upon the privacy of other individuals.
  - The information could compromise our business operations.
  - The request is assessed as vexatious or frivolous.
- Harbison provides reasons for denying or refusing access to personal information in writing. This correspondence will include information concerning the mechanisms for lodging a complaint.

Surveillance

The CEO will be responsible to ensure:

- Any devices in use are supplied by the Home. Members of the workforce are advised and supported to not use personal devices for surveillance. Members of the workforce are encouraged to report any matters of concern relating to the delivery of care and services to the RN in charge or supervisor.
- Any surveillance material stored electronically will be archived and destroyed as per this policy.

- Listening devices will not be used at the Home other than to record a conversation or meeting to which all parties consent, expressly or impliedly, to the listening device being used. Permission to use the device must be documented at the commencement of the meeting and stored with minutes of the meeting.
- Optical surveillance devices:
    - Cameras will only be used with the consent of resident/Person Responsible or member of the workforce. The camera will be a device supplied by Harbison. Personal cameras are not to be used under any circumstances. Examples of approved use of camera supplied by the Home may include:
        - Recording of clinical progress, e.g., wound healing.
        - Recording of social events for publishing in a newsletter.
    - CCTV is installed at the service and signage is installed on all external doors to advise all visitors to the service of the use of this device. CCTV is installed in common areas only, excluding bathrooms and change rooms.
- Safety devices**,** such as alert bands or anklets to aid in monitoring a resident's location and maintain their safety will only be used with the consent of the resident or their legal guardian**.** The Leadership Team will discuss the use of this device with the resident or Guardian and will record this conversation in Progress Notes and in the Care and Services Plan.
- Refer also to Work Health and Safety Policy and Procedures.

Quality and Correction of Personal Information

The CEO will be responsible to ensure:

- All reasonable steps are taken to ensure that the personal information Harbison collect, use, hold, or disclose is accurate, complete and up to date.
- Individuals have the right and ability to request that personal information Harbison holds is corrected if it is inaccurate, out of date, incomplete, irrelevant or misleading.
- All reasonable steps are taken to correct the personal information Harbison held.
- Harbison provides reasons for not complying with requests to correct personal information in writing.

Use of Government Issued Identifiers

The CEO will be responsible to ensure:

- We will not use government issued identifiers (a number assigned by a government agency to an individual as a unique identifier) for our operations.
- We will not use or disclose a government issue identifier assigned unless the use or disclosure is necessary to fulfil our organisational obligations (such as tax file numbers for employees) or is required under an Australian law or a court/tribunal

order (such as notifying the Aged Care Quality and Safety Commission (ACQSC) or NDIS Quality and Safeguards Commission of reportable incidents under the Serious Incident Response Scheme or NDIS Reportable Incident Scheme).

Anonymity

The CEO will be responsible to ensure:

- We will provide individuals the option of not identifying themselves, or of using a pseudonym, where it is lawful and practicable to do so.

Breaches of Privacy

Where a person believes that:

- A breach of this policy or
- The *Privacy Act*, or
- A gross breach of professional standards, in relation to privacy of a resident

has occurred, a written complaint should be made to the Privacy Officer (a designated position within the organisation). All complaints will be dealt with confidentially and promptly.

In addition, where the complaint involves a gross breach of privacy, e.g., where a worker has failed to perform their duties in line with relevant standards, and to the level a reasonable person would expect of them in their role, and their failure directly leads to harm to a resident's health or well-being including significant injury (physical, mental or emotional) or death, this must be reported to the ACQSC and NDIS Quality and Safeguards Commission (where the resident is a recipient of NDIS services in residential aged care). Refer to the reporting requirements in the Serious Incident Response Management and NDIS Reportable Incidents Policies and Procedures.

Notification

- Harbison will conduct an internal review where residents, families, friends or members of the workforce have complaints about how Harbison has dealt with personal information.
- An internal review may concern conduct where a person believes is:
    - A breach in information protection procedure.
    - A breach in the code.
    - An inappropriate disclosure by us of personal information.
    - Application for the internal review should be made in writing to the Privacy Officer. This application should be made within six months from the time the applicant became aware of the alleged breach or inappropriate disclosure.

- Complaints or incidents that involve potential 'neglect' of privacy standards or a gross breach of privacy, must be notified to the ACQSC within the timeframes as prescribed in the Serious Incident Response Management and NDIS Reportable Incidents Policies and Procedures (where the resident is a recipient of NDIS services). Where an incident is notifiable under the Serious Incident Response or NDIS Reportable Incident Schemes, an internal incident investigation must be conducted.

Nomination of Internal Review Team

In conducting an internal review under the *Privacy Act*, Harbison will nominate an investigation team within two weeks of receiving the compliant by the Privacy Officer.

Conducting the Privacy Review

The internal investigation team will take the following steps in conducting the review:

- Assist the applicant as much as possible.
- Apply the principles and the elements of the Open Disclosure framework to the investigation process.
- Interview relevant member/s of the workforce, examine records and obtain any other pertinent information on the circumstances of the alleged breach.
- Seek advice from court and legal service or from Office of the Australian Information Commissioner as required.
- Determine whether a breach of the *Privacy Act* has occurred and, if so, what harm or damage it has caused to the applicant.
- Prepare a report and submit the finalised investigation report to the Privacy Officer setting out the relevant facts, the conclusions reached and recommendations for action to be taken to resolve the complaint.
- If the outcome indicates a breach of the *Privacy Act* has been committed, the Privacy Officer will contact the Australian Information Commissioner regarding the finding and the corrective actions instituted.
- Indicate outcomes to the applicants and ensure that they are aware of the Office of the Australian Information Commissioner who can investigate privacy complaints from individuals about private sector organisations and government agencies.

Completion of Internal Review

- The internal review will be completed as soon as reasonably practicable and in a timeframe that is in keeping with the assessed risk and harm relating to the incident.
- If the review is not conducted with 60 days, the applicant can seek a review by the Privacy Officer.

- Once the review is completed, the Privacy Officer may decide to:
  - Take no further action on the matter.
  - Recommend a formal apology to the applicant.
  - Take appropriate remedial action.
  - Provide an understanding that the conduct will not occur again.
  - Implement measures to prevent recurrence of the conduct.

Contacting the Privacy Officer

- Our Privacy officer is:

  Name: Ashley Stoyles
  Contact Details: 02 4868 6208
- All stakeholders are encouraged to contact the Privacy Officer in relation to any privacy concerns or breaches.

Further Information

Additional information about the operational aspects of this policy can be obtained from our Privacy Officer. You can obtain further general information about your privacy rights and privacy law from:

Office	Contact Information
The Office of the Australian Information Commissioner	Phone: 1300 363 992 Website: www.oaic.gov.au Email: enquiries@oaic.gov.au Write to: The Office of the Australian Information Commissioner GPO Box 5218 Sydney NSW 2001
Aged Care Quality and Safety Commission	Phone: 1800 951 822 Website: www.agedcarequality.gov.au Email: info@agedcarequality.gov.au Write to: GPO Box 9819 Sydney 2000
NDIS Quality and Safeguards Commission	Phone: 1800 035 544 Website: www.ndiscommission.gov.au Email: contactcentre@ndiscommission.gov.au. Write to: PO Box 210 Penrith NSW 2750

RELATED DOCUMENTS

- Resident Privacy Agreement
- Privacy Register
- Request for Access to Personal Information Form
- Privacy Consent Form – External Services
- Workforce Confidentiality Agreement

RELEVANT LEGISLATION

- Aged Care Act 1997 (Cth)
- Australian Privacy Principles 2014 (Cth)
- Aged Care Quality Standards 2018 (Cth)
- Charter of Aged Care Rights 2019 (Cth)
- Australian Commission on Safety and Quality in Health Care. (2020) Informed consent in healthcare. Fact Sheet for Clinicians. Retrieved https://www.safetyandquality.gov.au/sites/default/files/2020-09/sq20-030_-_fact_sheet_-_informed_consent_-_nsqhs-8.9a.pdf
- National Disability Insurance Scheme (Incident Management and Reportable Incidents) Rules 2018 (Cth)
- National Disability Insurance Scheme (Provider Registration and Practice Standards) Rules 2018
- NDIS Quality and Safeguards Commission. (2021, November) NDIS Practice Standards and Quality Indicators, Version 4. Core Module. Outcomes:
    - 1.3 Privacy and Dignity
    - 1.4 Independence and informed choice
    - 2.2 Risk Management
    - 2.4 Information Management
    - 2.6 Incident Management
    - 2.7 Human Resources Management
    - 4.1 Safe environment
- Privacy Act 1988 (Cth)
- Privacy Amendment (enhancing Privacy Protection) Act 2012 (Cth)
- Quality of Care Principles 2014, Schedule 2: Aged Care Quality Standards:
    - Std 1 Consumer dignity and choice, Requirements (3) (e) (f)
    - Std 2 Ongoing assessment and planning with consumers, Requirements (3) (c) (d)
    - Std 3 Personal and clinical care, Requirements (3) (e)

- Std 4 Services and supports for daily living, Requirements (d)
- Std 5 Organisation's service environment (3) (b)
- Std 7 Human resources, Requirements (3) (c) (d)
- Std 8 Organisational governance, Requirement (3) (b) (c) (i) (v) (d)

- Reportable incidents: Detailed Guidance for Registered NDIS Providers, June 2019, NDIS Quality and Safeguards Commission
- Relevant State & Territory Privacy Acts
- Serious Incident Response Scheme: Guidelines for residential aged care providers, July 2022, Aged Care Quality and Safety Commission.
- Surveillance Devices Act 2007 (NSW)
- The Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth)