PRIVACY AND CONFIDENTIALITY POLICY AND PROCEDURE

Purpose and Scope

This policy and procedure sets out staff responsibilities relating to collecting, using, protecting and releasing personal information, in compliance with privacy legislation.

It applies to all:

- Our Caring Hearts staff;
- aspects of Our Caring Hearts' operations; and
- staff and participant personal information.

This policy and procedure should be read in conjunction with Our Caring Hearts' *Records and Information Management Policy and Procedure.* It meets relevant legislation, regulations and Standards.

Applicable NDIS Practice Standards

Information Management

Outcome

Management of each participant's information ensures that it is identifiable, accurately recorded, current and confidential. Each participant's information is easily accessible to the participant and appropriately utilised by relevant workers.

Indicators

- Each participant's consent is obtained to collect, use and retain their information or to disclose their information (including assessments) to other parties, including details of the purpose of collection, use and disclosure. Each participant is informed in what circumstances the information could be disclosed, including that the information could be provided without their consent if required or authorised by law.

- Each participant is informed of how their information is stored and used, and when and how each participant can access or correct their information and withdraw or amend their prior consent.

Privacy and Dignity

Outcome

Each participant accesses supports that respect and protect their dignity and right to privacy.

Indicators

- Consistent processes and practices are in place that respect and protect the personal privacy and dignity of each participant.

- Each participant is advised of confidentiality policies using the language, mode of communication and terms that the participant is most likely to understand.

- Each participant understands and agrees to what personal information will be collected and why, including recorded material in audio and/or visual format.

Interaction of Applicable Legislation and Associated Definitions

Privacy Act 1988 (Cth) - regulates how personal information about individuals is handled. The Act includes thirteen Australian Privacy Principles (APPs). The APPs set out standards, rights and obligations for the handling, holding, use, accessing and correction of personal information. The Act protects the privacy of an individual's information where it relates to Commonwealth agencies and private businesses (including not-for-profit organisations) with a turnover of more than $3 million. All organisations that provide a health service and hold health information (other than in a staff record) are covered by the Act.

Health Information – personal information or an opinion about:

- the health, including an illness, disability or injury, (at any time) of an individual;
- 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; or
  - 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.

Personal Information – information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- whether the information or opinion is true or not; and
- whether the information or opinion is recorded in a material form or not.

Sensitive Information – personal information or an opinion 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 orientation or practices;
- criminal record;

that is also:

- Personal Information;
- Health Information about an individual;
- genetic information about an individual that is not otherwise health information;
- biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
- biometric templates.

National Disability Insurance Scheme Act 2013 (Cth) – regulates how personal information about NDIS participants is handled by the National Disability Insurance Agency. This limits how the Agency collects and uses personal information and when and to whom information can be disclosed. The Agency must also comply with the Privacy Act 1988 (Cth).

Protected Information – information:

- about a person that is or was held in the records of the Agency; or
- to the effect that there is no information about a person held in the records of the Agency.

There is no information privacy law in South Australia. South Australian government agencies are required to comply with a set of Information Privacy Principles – PC012 Information Privacy Principles Instruction.

Personal Information - information or an opinion, whether true or not, relating to a natural person or the affairs of a natural person whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

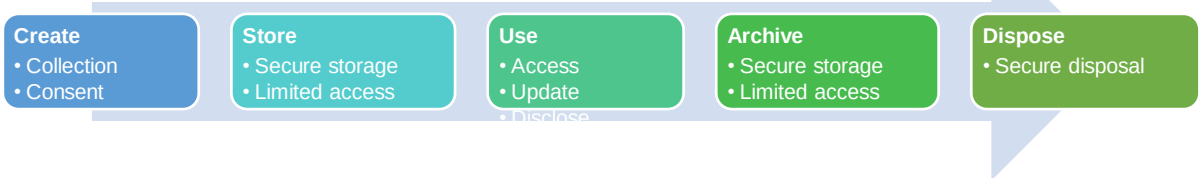
Private sector service providers must comply with the Privacy Act 1988 (Cth) when handling health information.
The Privacy Committee of South Australia oversees the implementation of the Information Privacy Principles by the South Australian public sector.
The Health and Community Services Complaints Commissioner receives complaints about government, private and non-government health and community services.

Policy

Our Caring Hearts recognises, respects and protects everyone's right to privacy, including the privacy of its participants and staff. All individuals (or their legal representatives) have the right to decide who has access to their personal information.

Our Caring Hearts privacy and confidentiality practices support and are supported by its records and information management processes (see the Records and Information Management Policy and Procedure).

Privacy and Confidentiality processes interact with the information lifecycle in the following ways:



All staff are responsible for maintaining the privacy and confidentiality of participants, other staff and Our Caring Hearts.

Procedures

General

The Human Resources is responsible for ensuring Our Caring Hearts complies with the requirements of the Privacy Act 1988 (Cth) as well as list any relevant legislation based on the list in 'Interaction of Applicable Legislation and Associated Definitions'. This includes developing, implementing and reviewing processes that address:

- why and how Our Caring Hearts collects, uses and discloses personal information;
- what information Our Caring Hearts collects about individuals and its source;
- who has access to the information;
- information collection, storage, access, use, disclosure and disposal risks;
- how individuals can consent to personal information being collected, withdraw or change their consent and change information about them held by Our Caring Hearts;
- how Our Caring Hearts safeguards and manages personal information, including how it manages privacy queries and complaints; and
- how information that needs to be updated, destroyed or erased is managed.

The Human Resources reviews these processes regularly, through annual Privacy Audits (see Our Caring Hearts' Privacy Audit Form and Schedule 2. External Audit and Internal Review Schedule).

All staff are responsible for complying with this policy and procedure and their privacy, confidentiality and information management responsibilities. Staff must keep personal information about participants, other staff and other stakeholders confidential, in accordance with the confidentiality provisions in their employment or engagement contract.

As per Our Caring Hearts' Human Resources Policy and Procedure, all staff must undergo Induction, which includes training in privacy, confidentiality and information management. Staff knowledge and application of confidentiality, privacy and information management processes is monitored on a day-to-day basis and through annual Performance Reviews. Additional formal and on-the-job training is provided to staff where required.
Our Caring Hearts' Privacy Statement prominently displayed in Our Caring Hearts premises and included in Our Caring Hearts' Participant Handbook and website.

A full copy of this policy and procedure must be provided upon request.

Photos and Videos

Photos, videos and other recordings are a form of personal information. Staff must respect people's choices about being photographed or videoed and ensure images of people are used appropriately. This includes being aware of cultural sensitivities and the need for some images to be treated with special care.

Information Collection and Consent

Participant Information Collection and Consent

Our Caring Hearts will only request personal information that is necessary to:

- assess a potential participant's eligibility for a service;
- provide a safe and responsive service;
- monitor the services provided; and
- fulfil government requirements for non-identifying and statistical information.

Personal client information that Our Caring Hearts collects includes, but is not limited to:

- contact details for participants and their representatives or family members
- details for emergency contacts and people authorised to act on behalf participants
- participants' health status and medical records
- medication records
- service delivery intake, assessment, monitoring and review information
- assessments, reviews and service delivery records
- external agency information
- feedback and complaints
- incident reports
- consent forms

Prior to collecting personal information from participants or their representatives, staff must explain:

- that Our Caring Hearts only collects personal information that is necessary for safe and effective service delivery;
- that personal information is only used for the purpose it is collected and is stored securely;
- what information is required;
- why the information is being collected and how it will be stored and used;
- the occasions when the information may need to be shared and who or where the information may be disclosed to;
- the participant's right to decline providing information;
- the participant's rights in terms of providing, accessing, updating and using personal information, and giving and withdrawing their consent; and
- the consequences (if any) if all or part of the information required is not provided.

Participants and their families must be provided with Our Caring Hearts' Privacy Statement and informed that a copy of this policy and procedure is available on request.

Staff must provide privacy information to participants and their families in ways that suit their individual communication needs. Written information can be provided in Easy English or explained verbally by staff. Staff can also help participants access interpreters or advocates where required.

After providing the above information, staff must use a Consent Form to:

- confirm the above information has been provided and explained; and
- obtain consent from participants or their legal representatives to collect, store, access, use, disclose and dispose of their personal information.

Participants and their representatives or families are responsible for:

- providing accurate information when requested;
- completing Consent Forms and returning them in a timely manner;
- being sensitive and respectful to other people who do not want to be photographed or videoed; and
- being sensitive and respectful of the privacy of other people in photographs and videos when using and disposing of them.

NDIS Audits

Our Caring Hearts complies with the requirements of the National Disability Insurance Scheme (Approved Quality Auditors Scheme) Guidelines 2018 whereby participants are automatically

included in audits against the NDIS Practice Standards. Participants may be contacted at any time by an NDIS Approved Quality Auditor for an interview, or for their participant file and plans to be reviewed.

Participants who do not wish to participate in these processes can notify any staff member, who must inform the Director in writing. Their decision will be respected by Our Caring Hearts and will be documented in their participant file. Upon commencement of any audit process, Our Caring Hearts notifies its Approved Quality Auditor of participants who have opted-out of the audit process.

Staff Information Collection and Consent

Personal staff information that Our Caring Hearts collects includes, but is not limited to:

- tax declaration forms
- superannuation details
- payroll details
- employment / engagement contracts
- personal details
- emergency contact details
- medical details
- NDIS Worker Screening Checks, Police Checks and Working with Children Checks
- qualifications
- First Aid, CPR, Anaphylaxis and other relevant certificates
- personal resumes

Where relevant, forms used to collect the above information will also obtain the staff member's consent to collect, store, access, use, disclose and dispose of their personal information.

Storage

Refer to the Records and Information Management Policy and Procedure for details on how Our Caring Hearts securely stores and protects staff and participant personal information.

Access

Staff personal information must only be accessed by the Director, who may only access the information if it is required in order to perform their duties.

Staff must only access participants' personal information if it is required in order to perform their duties.

Staff and participants have the right to:

- request access to personal information Our Caring Hearts holds about them, without providing a reason for requesting access;
- access this information; and
- make corrections if they believe the information is not accurate, complete or up to date.

All participant access or correction requests must be directed to a relevant staff member responsible for the maintenance of the participant's personal information. All staff access or correction requests must be directed to the Director within 2 working days of receiving an access or correction request, the responding staff member will:

- provide access, or explain the reasons for access being denied;
- correct the personal information, or provide reasons for not correcting it; or
- provide reasons for any anticipated delay in responding to the request.

An access or correction request may be denied in part or in whole where:

- the request is frivolous or vexatious;
- it would have an unreasonable impact on the privacy of other individuals;
- it would pose a serious threat to the life or health of any person; or
- it would prejudice any investigations being undertaken by Our Caring Hearts or any investigations it may be the subject of.

Any participant access or correction requests that are denied must be approved by the Director and documented on the participant's file.

Any staff access or correction requests that are denied must be approved by the Board of Directors and documented on the staff member's file.

Disclosure

Participant or staff personal information may only be disclosed:

- for emergency medical treatment;
- to outside agencies with the person's or for child participants, parent or guardians' permission;
- with written consent from someone with lawful authority; or
- when required by law, or to fulfil legislative obligations such as mandatory reporting.

If a staff member is in a situation where they believe that they need to disclose information about a participant or other staff member that they ordinarily would not disclose, they must consult the Director before making the disclosure.

Reporting

Notifiable Data Breaches Scheme

The Notifiable Data Breaches (NDB) Scheme is a national scheme that operates under the *Privacy Act 1988 (Cth)*. requires organisations to report certain data breaches to people impacted by the breach, as well as the Australian Information Commissioner.

A data breach occurs when personal information about others is lost or subject to unauthorised access. A data breach may be caused by malicious action, human error or a failure in information management or security systems.

Examples of data breaches include:

- loss or theft of devices (such as phones, laptops and storage devices) or paper records that contain personal information;
- unauthorised access to personal information by a staff member;
- inadvertent disclosure of personal information due to 'human error', for example an email sent to the wrong person; and
- disclosure of an individual's personal information to a scammer, as a result of inadequate identity verification procedures.

In addition to harm caused to people who are the subject of data breaches, an incident like this may also cause Our Caring Hands reputational and financial damage.

Further detail about the NDB Scheme is contained in the *Data Breach Preparation and Response - A Guide to Managing Data Breaches in Accordance with the Privacy Act 1988 (Cth)*, published by the Office of the Australian Information Commissioner (OAIC).

Our Caring Hearts *Data Breach Response Plan* outlines its strategy for containing, assessing and managing data breach incidents.

Identifying a Notifiable Data Breach

A Notifiable Data Breach, also called an 'eligible data breach', occurs when:

- there is unauthorised access to or disclosure of personal information, or information is lost in circumstances where unauthorised access or disclosure is likely to occur;
- the disclosure or loss is likely to result in serious harm to any of the people that the information relates to. In the context of a data breach, serious harm may include serious physical, psychological, emotional, financial, or reputational harm; and
- Our Caring Hearts has been unable to prevent the likely risk of serious harm through remedial action.

All potential or actual data breaches must be reported to the Director, who will determine Our Caring Hearts response and whether the breach needs to be reported under the NDB Scheme.

If Our Caring Hearts acts quickly to remediate a data breach and as a result it is not likely to result in serious harm, it is not considered a Notifiable Data Breach.

Responding to a Data Breach

If the Board of Directors suspects that a data breach is notifiable under the NDB Scheme, they must make an assessment to determine if this is the case.

If the Board of Directors believes that the data breach is notifiable under the NDB Scheme, they must notify Our Caring Hearts' Data Breach Response Team. This team comprises the:

- Manager as Team Leader, responsible for leading the response team and reporting to the Board of Directors;
- Manager as Project Manager, to coordinate the team and provide support to its members;
- Manager, to bring privacy expertise to the team;
- Director as legal support, to identify legal obligations and provide advice;
- Director as risk management support, to assess the risks from the breach;
- Human Resources as Information and Communication Technology (ICT) or forensics support, to help establish the cause and impact of a data breach that involves ICT systems;
- Human Resources to provide information and records management expertise, assist in reviewing security and monitoring controls related to the breach (for example, access, authentication, encryption, audit logs) and provide advice on recording the response to the data breach;
- Human Resources as Human Resources support, if the breach was due to the actions of a staff member; and
- Director to provide media/communications expertise and assist in communicating with affected individuals and dealing with the media and external stakeholders.

The Data Breach Response Team must notify all impacted individuals of the breach as soon as is practicable.

All data breach incidents (whether notifiable or not) must be responded to in accordance with Our Caring Hearts' *Data Breach Response Plan* and recorded in Our Caring Hearts' Incident

Register, with relevant actions tracked in its Continuous Improvement Register where appropriate.

Where a breach is referred to the Data Breach Response Team, its response will be based on the following steps:

- Step 1: Contain the data breach;
- Step 2: Assess the data breach and the associated risks;
- Step 3: Notify individuals and the Australian Information Commissioner; and
- Step 4: Prevent future breaches.

See Our Caring Hearts' *Data Breach Response Plan* for further detail.

Notifiable Data Breaches Involving More Than One Entity

The NDB Scheme recognises that personal information is often held jointly by more than one entity. For example, one entity may have physical possession of the information, while another has legal control or ownership of it.

Examples include:

- where information is held by a cloud service provider;
- subcontracting or brokering arrangements; and
- joint ventures.

In these circumstances, an eligible data breach is considered the responsibility of both entities under the NDB Scheme. However, only one entity needs to take the steps required by the NDB Scheme and this should be the entity with the most direct relationship with the people affected by the data breach. Where obligations under the Scheme (such as assessment or notification) are not carried out, both entities will be in breach of the Scheme's requirements.

Other Reporting Requirements

The Director must immediately notify the NDIS Commission and list any relevant complaints body in 'Interaction of Applicable Legislation and Associated Definitions' if they become aware of a breach or possible breach of privacy legislation.

Data breaches may also trigger reporting obligations outside of the *Privacy Act 1988*, such as to:

- Our Caring Hearts' financial services provider;
- police or other law enforcement bodies;
- the Australian Securities and Investments Commission (ASIC);
- the Australian Prudential Regulation Authority (APRA)
- the Australian Taxation Office (ATO);
- the Australian Transaction Reports and Analysis Centre (AUSTRAC);
- the Australian Cyber Security Centre (ACSC);
- the Australian Digital Health Agency (ADHA);
- Federal, State or Territory Government departments;
- professional associations and regulatory bodies; and
- insurance providers.

Archiving and Disposal

Refer to the Records and Information Management Policy and Procedure for details on how Our Caring Hearts archives and disposes of participants' personal information.

Supporting Documents

Documents relevant to this policy and procedure include:

- *Consent Form*
- *Records and Information Management Policy and Procedure*
- *Our Caring Hearts Information Sharing*
- *Data Breach Response Plan*
- *Continuous Improvement Register*
- *Participant Handbook*
- *Privacy Statement*
- *Privacy Audit Form*

Monitoring and Review

This policy and procedure will be reviewed at least every two years by the Boards of Directors. Reviews will incorporate staff, participant and other stakeholder feedback.

Our Caring Hearts feedback collection mechanisms, such as staff and participant satisfaction surveys, will assess:

- satisfaction with Our Caring Hearts' privacy and confidentiality processes;
- whether stakeholders have received adequate information about privacy and confidentiality; and
- the extent to which participants and their supporters feel their privacy and confidentiality has been protected.

Our Caring Hearts' Continuous Improvement Register will be used to record improvements identified and monitor the progress of their implementation. Where relevant, this information will be considered as part of Our Caring Hearts service planning and delivery processes.