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:

- Sync Space Therapy staff
- aspects of Sync Space Therapy's operations and
- staff and participant personal information.

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

National Requirements

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.

Privacy and Personal Information Protection Act 1998 (NSW) – regulates how personal information is handled by NSW public sector agencies including government agencies, local councils, State Owned Corporations, and universities.

Personal Information - information or an opinion (including information or an opinion forming part of a database and whether recorded in a material form or not) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. It includes such things as an individual's fingerprints, retina prints, body samples or genetic characteristics. It does not include any of the following:

- information about an individual who has been dead for more than 30 years
- information about an individual that is contained in a publicly available publication
- information about a witness who is included in a witness protection program under the *Witness Protection Act 1995* or who is subject to other witness protection arrangements made under an Act
- information about an individual arising out of a warrant issued under the *Telecommunications (Interception) Act 1979* of the Commonwealth
- information about an individual that is contained in a public interest disclosure within the meaning of the *Public Interest Disclosures Act 1994*, or that has been collected during an investigation arising out of a public interest disclosure
- information about an individual arising out of, or in connection with, an authorised operation within the meaning of the *Law Enforcement (Controlled Operations) Act 1997*
- information about an individual arising out of a Royal Commission or Special Commission of Inquiry

- information about an individual arising out of a complaint made under Part 8A of the *Police Act 1990*
- information about an individual that is contained in Cabinet information or Executive Council information under the *Government Information (Public Access) Act 2009*
- information or an opinion about an individual's suitability for appointment or employment as a public sector official
- information about an individual that is obtained about an individual under Chapter 8 (Adoption information) of the *Adoption Act 2000*
- information about an individual that is of a class, or is contained in a document of a class, prescribed by the regulations.

Health Records and Information Privacy Act 2002 (NSW) – regulates how health information is handled by NSW public sector agencies, public sector health organisations, private sector organisations, health service providers and businesses with a turnover of more than $3 million which hold health information.

Health information –

- personal information that is information or an opinion about:
    - the physical or mental health or a disability (at any time) of an individual
    - an individual's express wishes about the future provision of health services to him or her
    - a health service provided, or to be provided, to an individual or
- other personal information collected to provide, or in providing, a health service
- other personal information about an individual collected in connection with the donation or intended donation, of an individual's body parts, organs or body substances
- other personal information that is genetic information about an individual arising from a health service provided to the individual in a form that is or could be predictive of the health (at any time) of the individual or of a genetic relative of the individual or
- healthcare identifiers.

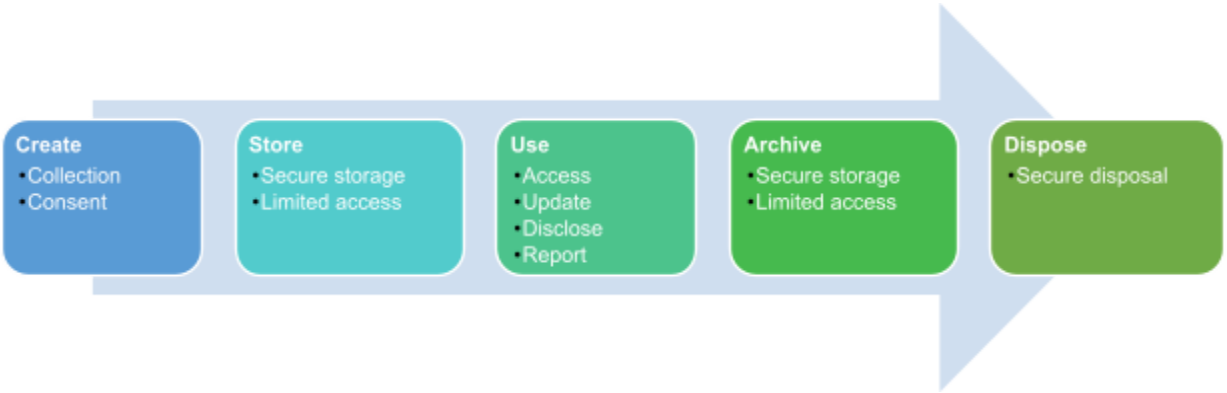
Private sector service providers in NSW must comply with the Privacy Act 1988 (Cth) and Health Records and Information Privacy Act 2002 (NSW) when handling health information. The NSW Information and Privacy Commission administers the HRIP Act and accepts complaints about health information.

Policy

Sync Space Therapy 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.

Sync Space Therapy's privacy and confidentiality practices support and are supported by its records and information management processes.

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 Sync Space Therapy.

Procedures

General

Sync Space Therapy's Privacy Officer is its Practice Manager. The Privacy Officer is responsible for ensuring Sync Space Therapy complies with the requirements of the *Privacy Act 1988 (Cth)* as well as National Disability Insurance Scheme Act 2013 (Cth), Privacy and Personal Information Protection Act 1998 (NSW) and Health Records and Information Privacy Act 2002 (NSW).

This includes developing, implementing, and reviewing processes that address:

- why and how Sync Space Therapy collects, uses, and discloses personal information
- what information Sync Space Therapy 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 Sync Space Therapy
- how Sync Space Therapy 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 Privacy Officer reviews these processes regularly, through annual Privacy Audits (see Sync Space Therapy's *Privacy Audit Form* and *the 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.

Sync Space Therapy's *Privacy Statement* can be found on the website and via a hyperlink on *Client Intake Form*. The *Privacy Statement* and a full copy of this policy and procedure will be provided upon request.

Photos and Videos

Photos, videos and other recordings are a form of personal information. This includes photos and videos taken for the purpose of service delivery and other purposes such as marketing and promotions. Staff must

- ensure the collection, storage, use, storage, and disposal of photos, videos, and other recordings comply with the requirements of this policy and procedure
- respect people's choices about being photographed or videoed
- ensure images or recordings of people are used appropriately and
- be 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

Sync Space Therapy 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
- fulfill government requirements for non-identifying and statistical information.

Personal client information that Sync Space Therapy 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
- NDIS plans, funding and billing information
- participants' health status and medical records
- medication and food intake records
- service delivery intake, assessment, monitoring and review information
- assessments, reviews and service delivery records
- external agency information
- feedback and complaints
- incident reports and
- consent forms.

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

- that Sync Space Therapy 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 representatives must be provided with Sync Space Therapy's *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 representatives 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 are responsible for:
- providing accurate information when requested
- completing *Consent Forms* and returning them in a timely manner
- being sensitive and respectful to 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.

Storage

Refer to the *Records and Information Management Policy and Procedure* for details on how Sync Space Therapy securely stores and protects staff and participant personal information.

Access

Staff personal information must only be accessed by the business owners and the Privacy Officer, 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 Sync Space Therapy 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 Privacy Officer. Within *5 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 Sync Space Therapy or any investigations it may be the subject of.

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

Any staff access or correction requests that are denied must be approved by the Privacy Officer 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 when applicable, the guardian's) 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 Privacy Officer 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.

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

Further detail about the NDB Scheme is contained on the Office of the Australian Information Commissioner (OAIC)'s website.

Sync Space Therapy's *Data Breach Response Plan* is currently under development and will be available in the future to outline its strategy for containing, assessing and managing data breach incidents.

Notifiable Data Breaches

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
- Sync Space Therapy has been unable to prevent the likely risk of serious harm through remedial action.

If Sync Space Therapy 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.

Detecting Data Breaches

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, for instance, a staff member browsing sensitive participant records without a legitimate purpose or a computer network being compromised by an external attacker resulting in personal information being accessed without authority
- unauthorised 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, because of inadequate identity verification procedures.

In reality, and particularly with respect to electronic data, data breaches can be difficult to detect. As such, all staff are responsible for:

- adhering to all Sync Space Therapy Policies, Procedures and processes relating to data creation, storage, use, archiving and disposal
- only transporting hard copy files and electronic storage devices in a secure, lockable container and with approval from the business owners or the Privacy Officer.
- implementing password protection and two-factor or multi-factor authentication on devices and software used to access Sync Space Therapy information

- ensuring all operating systems, browsers and plugins used on devices to access Sync Space Therapy information are up to date with patches and fixes and have appropriate security maintenance software installed and active and
- completely shutting down devices used to access Sync Space Therapy information at least once a week, to ensure updates are installed.

Reporting a Data Breach

All staff must report all potential or actual data breaches (including unusual activity in electronic systems and loss or theft of files or storage devices) as soon as possible to the Privacy Officer, who will determine Sync Space Therapy's response and whether the breach needs to be reported under the NDB Scheme.

Where a breach is identified, Sync Space therapy would respond 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.

If the Privacy Officer believes that the data breach is notifiable under the NDB Scheme, they must notify Sync Space Therapy's owners and all managers in order to delegate the following tasks:

- Reporting to the relevant governing body
- Seeking legal support as needed, to identify legal obligations and provide advice
- assessing the risks from the breach
- Seeking Information and Communication Technology (ICT) or forensics support, to help establish the cause and impact of a data breach that involves ICT systems
- Reviewing security and monitoring controls related to the breach (for example, access, authentication, encryption, audit logs)
- Communicating with affected individuals and external stakeholders.

Sync Space Therapy Team must notify all impacted individuals of the breach as soon as is practicable.

All data breach incidents must be recorded in Sync Space Therapy's *Incident Register* with relevant actions tracked in its *Continuous Improvement Plan* where appropriate.

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 Privacy Officer must immediately notify the NDIS Commission 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:

- Sync Space Therapy's 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 Sync Space Therapy archives and disposes of participants' personal information.

Supporting Documents

Documents relevant to this policy and procedure include:

- *Records and Information Management Policy and Procedure*
- *Data Breach Response Plan (currently under development)*
- *Consent Form*
- *Incident Register*
- *Continuous Improvement Plan*
- *Participant Handbook*
- *Privacy Statement*
- *Privacy Audit Form*

Monitoring and Review

This policy and procedure will be reviewed at least every two years by the management team of Sync Space Therapy. Reviews will incorporate staff, participant and other stakeholder feedback.

Sync Space Therapy's feedback collection mechanisms, such as staff and participant satisfaction surveys, will assess:

- satisfaction with Sync Space Therapy's 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.

Sync Space Therapy's *Continuous Improvement Plan* will be used to record improvements identified and monitor the progress of their implementation. Where relevant, this information will be considered as part of Sync Space Therapy's service planning and delivery processes.