Approved By:	Director	**Date Approved:**	October 2022
Review Date:	October 2024	**Version:**	2.2

Policy

Ability Health Solutions (AHS) is committed to protecting the privacy of personal and health information and ensuring information is kept securely.

AHS will comply with The Privacy Act 1988 and the Privacy Amendment Act 2012 to protect the privacy of individuals' personal information, and the Privacy and Data Protection Act 2014 (Victoria)

This includes having in place systems governing the appropriate collection, use, storage and disclosure of personal information, access to and correction and disposal of that information.

Outcome

- Compliance with legislative requirements governing privacy of personal information.
- All AHS clients/ participants are satisfied that their personal information is kept private and only used for the intended purpose

Ensuring all Staff Understand Privacy and Information Management Requirements

- The Director of AHS will review their Privacy Policy 2 yearly and ensure they understand their responsibility to protect the privacy of individuals' personal information.
- All Staff will undergo training related to Privacy and Information Management Requirements at the time of induction and then 2 yearly and cyber security yearly.

Definitions

- **Personal information** - means information (or an opinion) we hold (whether written or not) from which a person's identity is either clear or can be reasonably determined.

- **Sensitive information** - is a particular type of personal information - such as health, race, sexual orientation, or religious information.

Collection of Information

- AHS will receive and store personal information provided to us for the primary purpose of providing services to clients/ participants. Collecting information is necessary to ensure we can appropriately assess needs, provide a quality service, and comply with legal requirements.
- We will only collect the information we need to provide the relevant service.

- Client/ Participants are informed of the need to provide us with up to date, accurate and complete information.
- Staff will update the clinical record as soon as practical after the delivery of services &/or if notified of a change to ensure information is accurate and correct.
- Persons contacting AHS with an enquiry do not need to provide personal details. However, once a decision is made to progress to utilising AHS services, personal and sensitive information will need to be collected.

How we Collect Information

- AHS collects Personal Information in a variety of ways, including when clients/ participants interact with us electronically or in person, and when we provide services. If a client/ participant choose not to provide the information we believe is required, we may not be able to provide service.
- Information may be provided directly by the client/ participant or third party (i.e. relative, support coordinator, other health professional. Where we receive information from another service provider, we will assume that you have provided consent for the disclosure/sharing of all relevant information with your referring agency. If you do not consent to this or wish to have limitations placed on what information can be shared, you need to inform your treating therapist.

How information is Used and Disclosed

- The main purpose for which AHS collects, holds, uses and discloses personal information is so that we can deliver services and conduct our business activities and functions. This gives us the best opportunity to provide the appropriate level of service.
- AHS may need to share pertinent client/ participant information with other health professionals involved in a persons treatment, the referrer, funding body, relatives, guardian or legal representative. Information is only shared in order to provide the best service possible. Permission to share information is sought from the client/ participant prior to the delivery of services and as required at other points of intervention as / if required.
- Personal information is not disclosed to third parties outside of AHS, other than for a purpose made known to the client/ participant and to which they have consented, or unless required by law.
- When a client/ participant supplies information about themselves for a specific purpose, we will use the information only for that purpose, unless certain exceptions apply, such as where consent has been obtained or where it is reasonably expected to be used for a related purpose, to prevent a threat to life or health, in an emergency situation where the client/ participant may be at risk of harm and not able to provide consent, or to comply with a legal requirement such as a law, regulation, court order, subpoena, warrant, in the course of a legal proceeding or in response to a law enforcement agency request.

- AHS personnel including administrative staff, clinicians, management, as well as external contractors who maintain our clinical record management system have access to a client/ participants personal information.
- AHS refers to their Privacy & Information Management Policy on their website, and NDIS Service Agreement (NDIS participants), and available request.
- AHS uses a number of consent forms to assist in obtaining consent. These consents are discussed with clients/ participants and/or their decision maker in a way they can understand.

Information Storage and Security

- AHS will take reasonable steps to ensure personal information is protected from misuse, interference, loss, unauthorised access, modification or disclosure.
- Multi-factor Authentication is an additional security step to verify identity when logging into selected applications and systems. This extra layer of security protects from unauthorised access.
- All client details and records are confidential. AHS may hold information in either electronic or hard copy form (or both). Hard copies of any client/ participant specific documentation is scanned onto a client management system and then shredded.
- Client/ Participant information collected is kept in an individual client record.
- A client record includes: personal information • clinical notes • investigations • correspondence from other healthcare providers • photographs • video footage.
- Electronic health records are password protected on our client management system. When a staff member leaves AHS, their password access is ceased immediately.
- Non-electronic health records are kept in secure storage.
- Faxes containing any client related information are scanned onto our client management system by administrative staff and then shredded to ensure confidentiality.
- AHS staff are aware of the importance of strict confidentiality with respect to all communication both written and verbal.
- AHS takes reasonable steps to ensure the security of records when off-site and clinicians are aware of the importance of keeping records secure while travelling.
- AHS will destroy or permanently de-identify any information which is in its possession or control and which is no longer needed for the purpose for which it was collected provided AHS is not required under an Australian law or court/tribunal or otherwise to retain the information
- User access to all computers and mobile devices holding client/ participant information is managed by passwords and automatic inactive logouts.
- AHS uses technologies and processes such as access control procedures and passwords, network firewall, multi-factorial authentication and physical security to protect privacy.

- Client/ Participant information is stored for seven years post the date of last discharge. In the case of participants aged under 18 years, information is kept until their 25th birthday and 7 years post discharge.

Client/ Participant Access to Their Information

- Client/ Participants have the right to access the personal and health information AHS holds about them in accordance with the provisions of the Privacy Act 1988. A request can also be made to amend personal and health information should it believed to be inaccurate.
- A small administrative fee may be payable for the provision of information to cover the reasonable costs of supplying this information. The request to provide access to this information will be dealt with in a reasonable time.
- If a client/ participant would like a copy of the information about them which is held by AHS or believe that any information held is inaccurate, out of date, incomplete, irrelevant or misleading, contact can be made to admin@abilityhealthsolutions.com.au.
- AHS reserves the right to refuse to provide information that we hold about a client/ participant in certain circumstances as set out in the Privacy Act. In this situation, AHS will provide the reasons for refusal and inform the client/ participant of any exceptions relied upon under the Privacy Act.

Website Privacy

This Website Privacy Statement applies to the AHS website and online services.

Cookies

- When accessing the AHS website, we may also collect your personal information through the use of cookies. When you access our website, we may send a "cookie" (a small summary file containing a unique ID number) to your computer device. This enables us to recognise your device each time you visit our website. We may also use Google Analytics and other software (such as Javascript), or similar technology to measure traffic patterns, determine which areas of our website have been visited and to measure actions taken on our website such as form submissions. We use this to research website visitor behaviour so we can improve the experience. Our cookies do not collect personal information.
- If you do not wish to receive cookies, you can set your browser so that your device does not accept them. You can set your browser to notify you when you receive a Cookie and this will provide you with an opportunity to either accept or reject it in each instance. Please note that if you do this, it may affect some of the functions on our website.

Links

- Our website may contain links to other websites. Please note that when you click on one of these links, you are entering another site. We encourage you to read the privacy statements of these linked websites as their privacy policy may differ from ours as we do not accept responsibility for inappropriate use collection, storage or disclosure of you personal information outside of our site.

Privacy During Consultations & Communications

- Clinicians maintain minimum standards for privacy in addition to identifying and addressing each client's unique privacy needs. Needs may vary according to personal preference, natural modesty, the type of care being provided, the client's familiarity with the intervention and the place of intervention (e.g. home/ pool/ public place). AHS is a community-based provider only – as such, clinicians will continually address privacy issues with each client on an individual basis depending the environment.
- If treatment takes place in the client's home, clinicians ensure the client is comfortable with the location of treatment and close any doors or window coverings as required.
- If treatment is in a public place, clinicians communicate with the client to identify privacy needs and concerns e.g. client may not wish to walk down their local streets with a clinician or receive treatment in the open area of a care facility.
- If a client is required to disrobe for a particular intervention, the clinician provides a clear explanation of 'adequate undress' and the reason it is important. The clinician offers suitable cover (such as a towel or sheet) to protect the client's dignity. The clinician may turn their back or leave the room while a client disrobes.
- Where a client is particularly vulnerable and/or there is potential for the therapeutic relationship to be particularly sensitive, the clinician may seek the client's consent to have a third-party present if disrobing is required. This consent is documented in the client health record.
- Clinicians conduct discussions discreetly in person or over the telephone to respect client's privacy and protect their health information.
- Clinicians use the treatment rooms for telephone calls and discussions when available (or their mobile phone in an external private location).
- Team meetings are conducted in a private room or offsite to ensure adequate space and to maintain privacy.

Privacy in the AHS Office

Clinicians work environment ensures client confidentiality and privacy is maintained, including

- documents containing confidential information are not left unattended on printers or photocopiers
- the computer screen is locked
- documents are only printed when absolutely necessary
- confidential information is disposed of in the secure bin for shredding.

Information Security Precautions

General

- Access to all personal information is strictly based on a need-to-know basis
- Operating system updates ('patches') must be install promptly after they become available
- WiFi networks must have strong passwords to gain access
- Software only to be download or installed from trusted sources
- When an employee leaves, their access to the organisation's computer network and email system is removed promptly

Passwords

- All computers which store, or access personal information require unique & strong passwords
- Passwords must not be shared or reused between computers, users, or different applications
- Passwords should not be left written on paper left lying around
- Passwords should be regularly changed (and immediately if it becomes known by another person).
- Passwords should be strong passwords/ passphrases – they should not be easy-to-guess such as "123456", "password" etc.

Avoiding Scams and Ransomware

- Be aware of current scams targeting individuals & businesses by following government sites (i.e. SCAMWATCH)
- Be suspicious of any unsolicited emails or text messages purporting to be from government agencies, banks, delivery services, or other similar organisations – check the sender's email address for clues (scammers will try to fool you with a very similar email sender's address) and delete any suspicious emails or look up the organisation's main phone number and call if unsure
- Be suspicious of unsolicited phone callers purporting to be from Telstra, Microsoft, or the Australian Tax Office, and do not provide any information. Instead end the call – if unsure, look up their main number and call it to confirm
- Do not allow remote access to any computer or network resource by a third party unless it is arranged with a known and trusted IT services provider

Portable Devices

- Smart phones and mobile computers must not be left unattended in public, or in vehicles (locked or unlocked), or stored in checked-in baggage when flying.
- Portable storage devices (e.g. USB flash drives) should be checked for viruses prior to their use
- Portable storage devices require password protection if they are used to store any personal information (such as employee or participant information)

Social Media

- Only those authorised to do so should represent the organisation on social media
- Personal & confidential company information must not be posted or shared on social media

Printed Material

- Personal information in printed format must be stored securely when not being used, must not be left lying around, and when no longer required must be shredded or removed by a secure document destruction service.

Email security measures

- Only opening email attachments from trusted contacts and businesses.
- Blocking junk, spam and scam emails.
- Identifying, deleting and reporting suspicious looking emails.
- Knowing when it's appropriate to share your work email address.
- Must not permit other persons to use their account (other than through an email proxy arrangement or unless approved by the Director).

Incidents

- A data breach or breach of privacy and confidentiality is an incident, follow the Manage Incident and Cyber Security Response Plan process to manage and resolve the incident.
- Incidents where the individuals are at serious risk of harm as a result of the breach must be advised of the breach and assisted with ways to reduce their risk of harm from the breach.
- Incidents where individuals are at serious risk of harm as a result of the breach are reportable to the Office of the Australian Information Commissioner
- Serious risk of harm may include serious physical, psychological, emotional, financial, or reputational harm. Further, steps should be taken to prevent any further harm or damage.

Privacy Complaint or Concerns Management

If a person has a complaint regarding the way in which their personal information is being handled by AHS, in the first instance they are to contact the Director. The complaint will be dealt with as per the Complaints Management Policy. If the parties are unable to reach a satisfactory solution through negotiation, the person may request an independent person (such as the Office of the Australian Privacy Commissioner) or the NDIS Quality and Safeguards Commission to investigate the complaint. AHS will provide every cooperation with this process.

Contacting Ability Health Solutions regarding any concerns, queries or complaints:

- Post: Ability Health Solutions, PO BOX 2270,Oakleigh, VIC, 3166
- Email: admin@abilityhealthsolutions.com.au
- Phone: 9569 9941

Reference

- 'Guidelines on Privacy in the Private Health Sector', Office of the Australian Information Commissioner

Appendix 1: Summary of the 13 Australian Privacy Principles

APP 1 — Open and transparent management of personal information: Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

APP 2 — Anonymity and pseudonymity: Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

APP 3 — Collection of solicited personal information: Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive' information.

APP 4 — Dealing with unsolicited personal information: Outlines how APP entities must deal with unsolicited personal information.

APP 5 — Notification of the collection of personal information: Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

APP 6 — Use or disclosure of personal information: Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

APP 7 — Direct marketing: An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

APP 8 — Cross-border disclosure of personal information: Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

APP 9 — Adoption, use or disclosure of government related identifiers: Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier or use or disclose a government related identifier of an individual.

APP 10 — Quality of personal information: An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

APP 11 — Security of personal information: An APP entity must take reasonable steps to protect personal information it holds from misuse, interference, and loss, and from unauthorised access, modification, or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances**.**

APP 12 — Access to personal information: Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

APP 13 — Correction of personal information: Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.