

Privacy and Confidentiality Policy

1. Policy and Procedure

My Help is committed to protecting and upholding the right to privacy of clients, staff, volunteers, Governing body members and representative of agencies we deal with. In particular My Help is committed to protecting and upholding the rights of our clients to privacy in the way we collect, store and use information about them, their needs and the services we provide to them.

My Help requires staff and Governing body members to be consistent and careful in the way they manage what is written and said about individuals and how they decide who can see or hear this information.

My Help is subject to the *Aged Care Act, Schedule 2 User Rights Principles 2014* and will follow the guidelines of the *Australian Privacy Principles* in its information management practices. This policy will operate in conjunction with the organisation's *Records and Information Management Policy*.

My Help will ensure that:

- it meets legal and ethical obligations as an employer and service provider in relation to protecting the privacy of clients and organisational personnel
- clients are provided with information about their rights regarding privacy
- clients and organisational personnel are provided with privacy when they are being interviewed or discussing matters of a personal or sensitive nature
- all staff and Governing body members understand what is required in meeting these obligations.

This policy conforms to the *Privacy Act (1988)* (amended by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cwlth)*), and the *Australian Privacy Principles* which govern the collection, use and storage of personal information.

This policy will apply to all records, whether hard copy or electronic, containing

personal information about individuals, and to interviews or discussions of a sensitive, personal nature.

2. 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.

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.

Personal Information - information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) 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 in the course of 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 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.

3. Dealing with Personal Information

Information collected from a client may fit within two categories:

- a. Personal, safety, health and medical information; and
- b. Income information to determine if the client is experiencing personal financial hardship or will be subject to income testing (Home Care Packages only).

Personal information may include:

- Name
- Date of birth
- Gender
- Current and previous addresses

- Residency status
- Telephone numbers and e-mail addresses
- Financial information
- Bank account details
- Tax file number
- Driver's licence number
- Centrelink and my aged care information
- Photographs or videos
- Race or ethnicity
- Religion
- Care plan or progress notes
- Medical history or information provided by a health service.

Personal, safety, health and medical information is collected directly from the client, his/her relatives, other authorised people or services (e.g. Power of Attorney, General Practitioner, Aged Care Assessment Service, Hospitals) and through observations and assessments. This information is used to:

- Assess and provide services
- Administer and manage those services
- Evaluate and improve those services
- Ensure client safety
- Contact family, carers, or other third parties if required
- Meet our obligations under relevant legislation and aged care funding arrangements.

Information about the client's representatives and other contact persons is collected to:

- Enable sharing of information, as authorised by the client

- Register the person as a contact in case of emergency
- Enable regular/ongoing communications (if requested by the client).

In dealing with personal information, My Help staff will:

- Inform the client of what information is being collected, the purpose for collection, who will have access to the information, their rights to seek access to, and/or correct the information, and the right to make a complaint or appeal decisions about the handling of their information
- Ensure privacy for consumers, staff and governing body members when they are being interviewed or discussing matters of a personal or sensitive nature
- Only collect and store personal information that is necessary for the functioning of the organisation and its activities
- Use fair and lawful ways to collect personal information
- Ensure that people know what sort of personal information is held, what purpose it is held for and how it is collected, used, disclosed and who will have access
- Ensure that personal information collected or disclosed is accurate, complete and up-to-date, and provide access to any individual to review information or correct wrong information about themselves
- Take responsible steps to protect all personal information from misuse and loss and from unauthorised access, modification or disclosure
- Destroy or permanently de-identify personal information no longer needed and/or after legal requirements for retaining documents have expired

4. Responsibilities for Managing Privacy

- All staff are responsible for the management of personal information to which they have access, and in the conduct of research, consultation or advocacy work.
- The Director is responsible for content in My Help publications, communications and web site and must ensure the following:

- appropriate consent is obtained for the inclusion of any personal information about any individual, including My Help personnel
 - information being provided by other agencies or external individuals conforms to privacy principles
 - that the website contains a Privacy statement that makes clear the conditions of any collection of personal information from the public through their visit to the website
- The CEO is responsible for safeguarding personal information relating to My Help staff and Governing body members, volunteers, contractors, and My Help members
- The CEO works with the Privacy Officer who is responsible for:
 - ensuring that all staff are familiar with the Privacy Policy and administrative procedures for handling personal information
 - ensuring that clients and other relevant individuals are provided with information about their rights regarding privacy
 - handling any queries or complaints about a privacy issue

5. Privacy Information for Clients

At the initial assessment clients will be told what information is being collected, how their privacy will be protected and their rights in relation to this information. The information will be outlined in their Home Care Agreement and also in the Client Information Handbook.

The *Privacy and Confidentiality Brochure* and *Client Consent Form* is to be provided to clients at the time of commencing services with My Help. This form is to be:

- Signed and placed in the client's file; and
- Held securely with access limited to staff members in the performance of their role.

Clients, their families and carers will be encouraged to provide feedback on My Help's privacy practices in our quarterly Client Satisfaction Survey.

6. Updating Participant Information

To ensure that client information is accurate, complete, current, relevant and not misleading, My Help checks personal details and updates participant files accordingly:

- whenever reviewing a client's service; and / or
- upon being informed of changes or inaccuracies by clients or other stakeholders

There will be no charge for any correction of personal information.

Where My Help has previously disclosed client personal information to other parties, should the client request us to notify these parties of any change to their details, we must take reasonable steps to do so.

7. Collection and Storage of Personal Information

My Help collects information:

- directly from clients orally or in writing
- from third parties, such as medical practitioners, government agencies, client representatives, carer/s, and other health service providers
- from client referrals; and
- from publicly available sources of information.

My Help will collect sensitive information:

- only with client consent, unless an exemption applies (e.g. the collection is required by law, court/tribunal order or is necessary to prevent or lessen a serious and imminent threat to life or health)
- fairly, lawfully, and non-intrusively
- directly from the client, if doing so is reasonable and practicable
- only where deemed necessary to support

My Help takes all reasonable steps to protect personal information against loss, interference, misuse, unauthorised access, modification, or disclosure. My Help will destroy, or permanently de-identify personal information that is:

- no longer needed
- unsolicited and could not have been obtained directly
- not required to be retained by, or under, an Australian law or a court/tribunal order.

My Help has appropriate security measures in place to protect stored electronic and hard-copy materials, including secure filing systems in locked cabinets, with access restricted to appropriate staff and password protected electronic records systems.

My Help has an archiving process for client files which ensures files are securely and confidentially stored and destroyed in due course (see *Records and Information Management Policy*).

Should a breach in privacy occur, potentially exposing client information (e.g. computer system hacked, laptop stolen etc.) the Director will immediately act to rectify the breach in accordance with organisational policy and processes (see Breaches of Privacy, below).

8. 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.

9. Disclosing Information

My Help respects the right to privacy and confidentiality, and will not disclose personal information except:

- where disclosure would protect the client and / or others
- where necessary for best service practice
- where obligated by law.

For these purposes, My Help may disclose clients' personal information to other people, organisations or service providers, including:

- medical and allied health service providers who assist with the services we provide to clients
- a 'person responsible' if the client is unable to give or communicate consent (e.g. next of kin, carer, or guardian)
- the client's authorised representative/s (e.g. legal adviser)
- our professional advisers (e.g. lawyers, accountants, auditors)
- government and regulatory authorities (e.g. Centrelink, My Aged Care, government departments, and the Australian Taxation Office)
- organisations undertaking research where information is relevant to public health or public safety
- when required or authorised by law.

10. International Disclosure

Under the Privacy Act 1988, before My Help discloses personal information to an overseas recipient, it must take reasonable steps to ensure the overseas recipient does not breach the Principle 8 of the Australian Privacy Principles (APPs).

The CEO is responsible for undertaking these investigations.

This requirement does not apply if:

- the overseas recipient is subject to a law or binding scheme that has the effect of protecting the information in a way that is substantially similar to protection given under the APPs, and
- there are mechanisms available to enforce that protection.

11. Accessing Personal Information

Clients can request and be granted access to their personal information, subject to exceptions allowed by law. Access to health information can be arranged and are guided by the relevant Health Privacy Principles and Acts in each state.

Requests to access personal information must state:

- the information to be accessed
- the preferred means of accessing the information,
- and should be forwarded to the Privacy Officer either verbally, or in writing.

The Privacy Officer and Directors will assess the request to access information, taking into consideration current issues that may exist with the client, and whether these issues relate to any lawful exceptions to granting access to personal information.

Should it be decided that access to personal information will be denied, the Privacy Officer must, within 20 business days of receipt of the request, inform the client in writing of:

- the reasons for denying access and
- the mechanisms available to complain or appeal.

Should access be granted, the Privacy Officer will contact the client within 20 business days of receipt of the request to arrange access to their personal information.

Should My Help be unable to provide the information in the means requested, the Privacy Officer will discuss with the client alternative means of accessing their personal information.

Reasonable charges and fees, incurred by My Help in providing the data as requested, may be passed on to the client.

12. Complaints

Questions or concerns about My Help's privacy practices should be brought, in the first instance, to the Director's attention.

In investigating the complaint, My Help may, where necessary, contact the client making the complaint to obtain more information.

The client will be advised either in writing, or in a face-to-face meeting, of the outcomes and actions arising from the investigation.

If concerns cannot be resolved and a client wishes to formally complain about how

their personal information is managed, or if they believe My Help has breached an APP and/or IPP, they may send their concerns in writing to:

Office of the Victorian Information Commissioner for Privacy and Data Protection

121 Exhibition Street

Melbourne VIC 3000

Telephone: 1300 666 444

Email: enquiries@ovic.vic.gov.au

13. Breaches of Privacy

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.

To prevent or address a data breach or breach of privacy, the following process are in place:

Establish the Data Breach Response Team

The Data Breach Response Team will include:

Privacy Officer: The Privacy Officer, designated as the Aged Care Services Coordinator, is responsible for overseeing the breach response, ensuring compliance with data protection regulations, coordinating with legal counsel, and assessing the potential impact on personal data.

Incident Response Coordinator (IRC): The Incident Response Coordinator, who will be assigned based on the type of breach and the expertise required, is tasked with overall coordination of the data breach response process, acting as a liaison with senior management and legal counsel, and ensuring adherence to the response plan.

IT Security Adviser: The IT Security Adviser may be the Director, internal IT Manager, external IT Consultant or the lead security personnel of the system which has experienced the breach. They take the lead in the technical aspects of data breach

detection and response, coordinate with the team to isolate and contain breaches, and assist with investigations.

Public Relations/Communications: The Public Relations/Communications officer (may be an internal or external resource), manages internal and external communications during data breaches, prepares public statements and communications with clients, and handles media inquiries.

Legal Counsel: The Legal Counsel (which may be internal or an external advisor), provides legal guidance throughout the data breach response process and ensures compliance with relevant laws and regulations.

Implement the Incident Response Plan

My Help is responsible for creating a comprehensive data breach response plan, outlining roles, and responsibilities, as well as defining severity levels of data breaches and corresponding responses.

The plan will include the identification of all sensitive data handled by My Help, such as personal health information, financial data, and personal identifiers. This plan will be followed in the event of a breach.

Implement Security Measures

My Help ensures the implementation of robust security measures, including encryption, access controls, and regular security audits.

Data Breach Detection

My Help implements intrusion detection systems and real-time monitoring to promptly identify potential breaches. Staff members are educated about recognising and reporting unusual activities or suspicious behaviour.

Any staff who identify a potential breach must immediately inform their line manager, who must report to the Director for further action.

If a staff member is suspected to have breached privacy, a thorough investigation will be undertaken to determine the exact nature of the breach, and a response made appropriate to the situation (e.g. serious disciplinary actions or termination or employment).

Further detail about the Notifiable Data Breaches (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).

Data Breach Classification

The Incident Response Plan defines a classification system to assess the severity of data breaches based on the type and amount of compromised data.

Containment and Mitigation

In case of a detected breach, My Help will isolate affected systems and networks to prevent further damage and address the vulnerability that led to the breach.

Notification Requirements

The Incident Response Plan ensures understanding and compliance with obligations under the Notifiable Data Breaches (NDB) scheme. It mandates the preparation of templates for breach notification letters and public statements.

Legal and Regulatory Compliance

Legal counsel is consulted to ensure compliance with Australian data protection laws, and potential legal and financial consequences of data breaches are understood.

Public Relations and Communication

A communication plan is created to address internal and external stakeholders, and coordination with public relations experts is outlined to manage the organisation's public image during and after a breach.

Data Breach Documentation

The Incident Response Plan mandates the maintenance of comprehensive records of data breaches, including timing, scope, containment efforts, and notifications sent.

Remediation and Prevention

A plan for remediating the effects of a breach and preventing future breaches is developed. Employee training programs on data security best practices are also implemented.

Reviews and Updates

Regular reviews and updates of the data breach response plan are conducted to incorporate lessons learned from previous incidents and changes in regulations.

Testing and Training

Regular tabletop exercises are conducted to test the effectiveness of the response plan. Employees are trained on their roles and responsibilities in case of a breach.

Reporting to Authorities

My Help are required to disclose a data breach to the Office of Australian Information Commissioner if the data contains personal information that is likely to result in “serious harm”, which includes any of the following: physical, psychological, financial or reputational harm. Personal information is information about an identified individual, or an individual who is reasonably identifiable.

Third-Party Relationships

The plan emphasises the importance of third-party service providers having robust data security measures and a breach response plan.

Insurance

Consideration of cyber insurance to mitigate the financial impact of a data breach is encouraged.

14. Supporting Documents

Relevant documents relating to this Policy and Procedure:

- Records and Information Management Policy
- Client Information Handbook
- Client Consent Form