

Think Mental Health Community Services

# Privacy Policy



## Contents

1. Purpose .....	3
2. Personal information .....	3
2.1 Storage of personal information .....	3
2.2 Collection of personal information.....	3
2.3 Purpose of holding personal information.....	4
2.4 Accessing personal information .....	4
3. Confidentiality of information .....	4
3.1 Exceptions to confidentiality .....	4
4. Data breach policy .....	5
5. Requests for access and correction to client information .....	5
6. Complaints and concerns.....	5

Record of policy development:

Version number	Date of issue	Lead author/reviewer	Consultative panel	Significant changes on previous version
1	05/11/2025	Jacinta Essam	Think Mental Health Management Team	Nil, first version

*Think Mental Health acknowledges the Traditional custodians on the land on which we live and work, and of the many different nations across the wider regions from which we all come. In Canberra this is the Ngunnawal people.*

*We pay our respects to the Elders past, present and emerging as the holders of the memories, the traditions, the culture and the spiritual wellbeing of the Aboriginal and Torres Strait Islander peoples across the nation.*

## 1. Purpose

Think Mental Health (TMH) delivers various Government funded, community sector health services. TMH provides quality health care that is individually tailored and delivered by assigned health and wellbeing professionals. Staff across the community sector services include; admin support, counsellors, mental health assistants, registered nurses, occupational therapists, psychologists, psychiatrists, peer workers, social workers and social and emotional wellbeing workers.

This policy applies to all individuals whose personal information is collected, used, or stored by Think Mental Health Clinic while delivering health services. All staff employed across Think Community Services are bound by the legal requirements of the Australian Privacy Principles set out in the Privacy Act 1988 (Cth) and Health Records (Privacy and Access) Act 1997.

## 2. Personal information

### 2.1 Storage of personal information

All information is stored securely and accessed only by those authorised to access the information, in accordance with clinic policies and procedures.

Information is stored using an electronic client management platform.

The information collected includes personal details such as name, address, and contact phone numbers. As part of the provision of health services, additional personal information relevant to the presenting concerns will also be collected and recorded. This may include records of session content, test material, results of any tests or assessments undertaken, and information provided by third parties such as medical specialists, general practitioners, other government, community or private sector services.

### 2.2 Collection of personal information

Personal information may be collected in the following ways:

- When information is provided directly to the treating health professional, whether verbally or in writing (e.g. letters, emails, text messages);
- During interaction with Think staff, including administration personnel;
- Through referrals, correspondence, and reports from other health practitioners, such as general practitioners;
- From third parties such as public, community or private sector services.

Concerns regarding the accuracy of recorded information should be directed to the administration team or the treating health professional. Clarification regarding how personal information has been collected or recorded can be requested by a consumer at any time.

## 2.3 Purpose of holding personal information

Personal information is collected and retained to support the provision of high quality, safe health services. This includes documenting initial assessment, any interventions provided, recovery goals, progress towards goals, clinical and general observations, attendance and engagement with various parts of the services. These records support accurate and appropriate delivery of services, and fulfill ethical, professional, and legal record-keeping requirements. Without this information, it may not be possible to provide appropriate or safe health services.

## 2.4 Accessing personal information

Access to personal information held on file may be requested at any time. Requests can be made verbally or in writing. In accordance with the *Privacy Act 1988 (Cth)*, access will be granted unless there are legal exceptions that restrict or prevent disclosure.

All written requests for access will be responded to in writing within 30 days. Where appropriate, an appointment may be arranged to provide clarification or support in reviewing the requested information.

# 3. Confidentiality of information

Personal information gathered during the provision of health services is treated as confidential and is not disclosed except under certain circumstances. In most cases, information will only be shared with the client's written consent.

Consent will be sought for disclosure in the following situations:

- Sharing information with a family member, guardian, or carer;
- Discussing relevant matters with third parties, such as general practitioners, employers, or agencies involved in funding the service;
- Providing written reports regarding assessment or treatment to other professionals or agencies, including general practitioners, medical specialists, legal representatives, schools and universities;
- Disclosing information in any other manner not explicitly referenced within this policy.

All Health Professionals are also required to engage in professional supervision and peer consultation; this is part of the quality assurance process. In such cases, personal information may be discussed in a de-identified format to protect anonymity, ensuring that individuals cannot be identified.

## 3.1 Exceptions to confidentiality

In certain circumstances, personal information may be disclosed without consent. These exceptions are limited and occur only when required or authorised by law, or when there is a serious risk to safety. These situations include:

- When a court issues a subpoena or disclosure is otherwise required or authorised by law;
- When mandatory reporting obligations apply, such as reporting concerns related to child protection or abuse;
- When there is a reasonable belief that a person is at risk of serious harm to themselves or others, and disclosure is necessary to prevent that harm.

In such cases, only the information relevant to the specific situation will be disclosed, and all reasonable steps will be taken to maintain the privacy and dignity of the individuals involved.

#### 4. Data breach plan

In the event of unauthorised access, disclosure, or loss of personal information, Think Mental Health Community Services will activate its data breach response plan as set out in the *Code of Conduct* and take all reasonable steps to minimise the risk of serious harm.

#### 5. Requests for access and correction to client information

At any time, a request may be made to access or correct the personal information held on file. The treating Health Professional may discuss the contents of the file with the individual and/or provide a copy, subject to the exceptions outlined in the *Privacy Act 1988 (Cth)*.

If it is determined that the personal information held is inaccurate, out of date, or incomplete, reasonable steps will be taken to correct it in a timely and appropriate manner.

Requests for access to or correction of personal information can be made directly to the worker involved or to the service's administrative staff. All written requests will be responded to in writing within 30 days, and an appointment may be arranged if further clarification or discussion is required.

#### 6. Complaints and concerns

Any concerns regarding the management of personal information can be raised with the worker involved or reception staff. Individuals are encouraged to raise any questions, complaints, compliments, or suggestions in line with the service's Complaints, Compliments and Suggestions Policy.

Upon request, a copy of the Australian Privacy Principles can be provided. These principles outline individuals' rights and describe how personal information should be handled.

If a concern cannot be resolved within the service involved, or if a formal complaint is preferred, it can be lodged with the Office of the ACT Human Rights Commission, the Health Services Commissioner can deal with complaints regarding all Health Services delivered within the ACT. The Commission is contactable on:

- Phone: (02) 6205 2222
- Online: [Contact Us - HRC](#)
- Email: [human.rights@act.gov.au](mailto:human.rights@act.gov.au)
- Mail: GPO Box 158 Canberra ACT 2601