Privacy and Confidentiality Policy	
Application	All parts of Thorne Harbour Health including all board members, employees, volunteers, students on placement
Exceptions	No exceptions
Legal and regulatory framework	Privacy Act 1988 (Cth) incorporating the Notifiable Data Breaches Scheme Health Records Act 2001 (Vic) Information Privacy and Data Protection Act 2014 (Vic) Freedom of Information Act 1982 (Vic) Fair Work Act 2009 (Cth) My Health Records Act 2012 (Cth)
Standards	QIC Standards (7th ed): 2.2 Human resources, 2.4 Knowledge management, 3.2 Consumer and community involvement (3.2.4), 5.2 Focusing on positive outcomes (5.2.5) Human Services Standards: 1 Empowerment RACGPS Standards (5th ed): Standard C6.3 Confidentiality and privacy of health and other information; C6.4 Information Security; GP2.3 Engaging with other services
Contractual agreements	DHHS funding and service agreement
Associated policies and procedures	Client Confidentiality Procedure Notification of Privacy Breaches Work Instruction Complaints, Compliments and Suggestions Procedure Penelope (CMS) instructions
Associated templates or forms	Individual service consent forms Thorne Harbour Health Staff & Volunteer Confidentiality Agreement
Other associated documents	Thorne Harbour Health Privacy Statement Volunteer Handbook – Privacy & Confidentiality Staff Code of Conduct Volunteer Code of Conduct

1. Purpose

Thorne Harbour Health has a legal and ethical obligation to protect and uphold the right to privacy of our clients and their families, Thorne Harbour Health members, employees, volunteers, board members, students and representatives of agencies and organisations with which we deal, and to maintain the confidentiality of the personal, health and sensitive information we hold about them.

The *Privacy and Confidentiality Policy* outlines Thorne Harbour Health's commitment to meeting these obligations and how this will be achieved.

This version of the policy (version 2.00) incorporates changes triggered by:

- The introduction of the *Notifiable Data Breaches (NDB) Scheme* which sits under the umbrella of the *Privacy Act 1988 (Cth)* which applies to all parts of Thorne Harbour Health including those in other jurisdictions, and
- A requirement that services funded by the Victorian Department of Health and Human Services report breaches of the privacy of DHHS-funded clients to the Department.

2. Scope

All Thorne Harbour Health employees, consultants, volunteers, students on placement and the board must comply with this *Privacy and Confidentiality Policy*.

The *Privacy and Confidentiality Policy* applies to all personal, health or sensitive information about individuals collected, used, stored, disclosed, shared and destroyed by Thorne Harbour Health, regardless of the format of the information (recorded or not recorded, in hard-copy or electronic format, in printed, audio, or visual form, web-based or on social media, or in any conversation or discussion).

All privacy-related Thorne Harbour Health procedures, work instructions and other guiding documents and information are to comply with this *Privacy and Confidentiality Policy*.

Confidentiality of organisational information is covered by the *Staff Code of Conduct*.

3. Definitions

Confidentiality is a separate legal concept to *privacy*. *Confidentiality* applies to information given to a person or organisation under an obligation not to disclose that information to others unless there is a statutory requirement or duty of care obligation to do so. *Confidentiality* also applies to organisational information which is not to be used or disclosed by board members, staff, volunteers, contractors or students without authorisation.

Employee refers to any person employed in a paid position at Thorne Harbour Health (whether permanent, temporary, casual, sessional, or on a short-term contract).

Health information refers to any information relating to a person's physical, mental or psychological health or disability.

Privacy refers to keeping certain personal information free from public knowledge and attention and to having control over its disclosure and use.

Personal information refers to any information that may identify a person. Personal information includes a person's name or address, and can include photos, credit history information, bank details, where a person works and any other information that could reasonably identify them.

Sensitive information may refer to information including a person's race, ethnicity, political opinions, membership of political associations and trade unions, religious or philosophical beliefs, sexual preferences, health and genetic information or criminal records.

Volunteer refers to any person formally engaged by Thorne Harbour Health to undertake tasks for which they are not paid.

4. Policy Statement

Thorne Harbour Health will protect and uphold the right to privacy of our clients and their families, Thorne Harbour Health members, employees, volunteers, board members, and representatives of agencies and organisations we deal with.

All Thorne Harbour Health employees, volunteers, board members and students on placement are 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.

Thorne Harbour Health will meet its legal and ethical obligations as an employer and service provider to protect the privacy of people and the confidentiality of their information.

As a community service provider, Thorne Harbour Health has a special obligation to protect and uphold the right to privacy and confidentiality of our clients. All employees, volunteers, students,

board members and contractors are required to follow the procedure provided in the *Client Confidentiality Procedure*.

Thorne Harbour Health will monitor compliance with our *Privacy and Confidentiality Policy* and be externally assessed against the privacy and confidentiality criteria set forth in relevant quality standards.

Thorne Harbour Health's *Privacy and Confidentiality Policy* will be implemented through the *Client Confidentiality Procedure*, the *Client Access to Client Care Records Procedure* and the *Notification of Privacy Breaches Work Instruction*, to ensure that:

- The *Privacy and Confidentiality Policy* is available on request in an appropriate format and publicly available via the Thorne Harbour Health website
- The quality of the personal, health and sensitive information we collect, hold, use, share and disclose is maintained
- Clients, employees, volunteers, board members, contractors and students (and applicants for any of such roles or Thorne Harbour Health services) are provided with privacy when they are being interviewed or discussing matters of a personal or sensitive nature
- All employees, volunteers, board members and contractors are informed of their obligations under the Thorne Harbour Health *Privacy and Confidentiality Policy*
- Any personal, health or sensitive information is collected only if needed for a specified primary purpose
- People know why we collect this information and how we will handle it
- The information is used and disclosed only for the primary purpose it was collected or a directly related purpose, or for another purpose only with the person's informed consent, unless otherwise prescribed or permitted by law. Permitted disclosure includes that necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety

  (Refer below to section *6.1 Legislative compliance*)
- Information is stored securely, and protected from misuse, loss and unauthorized access or modification
- Information is retained for the period required by the *Health Records Act 2001* and then safely destroyed
- Clients have access to information about their rights regarding privacy and confidentiality, including their right to complain if they feel there has been a breach, and their right to access their information and make corrections
- Clients are provided with details of whom they can contact should they feel their privacy has been breached, including where to go for external advice or advocacy support
- Privacy and confidentiality-related complaints and breaches are effectively dealt with through fair and consistent procedures. Refer to:
  - *Complaints, Compliments and Suggestions Procedure*
  - *Volunteer Grievance and Disciplinary Procedures*
  - *BPM-004 Addressing Conflict, Grievance and Complaints Policy* (board)
  - *Disciplinary Policy and Procedures*
  - *Thorne Harbour Health's Constitution* - s43 Disputes and Mediation (members)

- *Notification of Privacy Breaches Work Instruction*

5. Roles and Responsibilities

Ultimate responsibility for ensuring compliance with Thorne Harbour Health's *Privacy and Confidentiality Policy* and associated procedures sits with the President at the board level and with the CEO at the operational level.

Team leaders and supervisors have a responsibility to ensure that their staff, volunteers and students on placement, whose work they supervise or monitor, are complying with this policy and associated procedures.

Thorne Harbour Health board members, employees, volunteers and students on placement have a responsibility to comply with this policy and associated procedures.

Thorne Harbour Health will appoint a Privacy Officer who will be responsible for:

- ensuring that all employees and volunteers are familiar with the Privacy and Confidentiality Policy and procedures for handling personal information
- ensuring that clients and other relevant individuals are provided with information about their rights regarding privacy and confidentiality
- handling queries or complaints about a privacy or confidentiality issue

6. Legislative and contractual compliance

6.1 Legislative compliance

Thorne Harbour Health will comply with the following legislation:

- *Privacy Act 1988* (Commonwealth) incorporating the *Notifiable Data Breaches Scheme*
- *Health Records Act 2001* (Victoria)
- *Information Privacy and Data Protection Act 2014* (Victoria)
- *Freedom of Information Act 1982* (FoI Act) (Victoria)
- *Fair Work Act 2009* (Commonwealth)

All Thorne Harbour Health employees, contractors, volunteers and members of the board will adhere to the following privacy principles inherent in the above legislation.

- *Australian Privacy Principles (*Commonwealth) ('APP')
- *Health Privacy Principles* (Victoria) ('HPP')
- *Information Privacy Principles* (Victoria) ('IPP')

These principles are summarised in Attachment 1.

Collectively, these Acts, and the privacy principles therein, underpin how Thorne Harbour Health manages the personal, health and sensitive information the organisation holds or that has been disclosed to Thorne Harbour Health employees, contractors, volunteers and members of the board. Note that other legislation, such as the *My Health Records Act 2012* (Cth), may have implications for the privacy and confidentiality of the personal, health and sensitive information held by Thorne Harbour Health.

Refer to Thorne Harbour Health *Notification of Privacy Breaches Work Instruction* for further details.

6.2 DHHS Privacy Incident Report

As an organisation funded by the Victorian Department of Health and Human Services (DHHS), Thorne Harbour Health is required to immediately notify DHHS when becoming aware of a breach of

the privacy of a DHHS-funded client, or a possible breach, as defined under the *Privacy and Data Protection Act 2014 (Vic)* or the *Health Records Act 2001 (Vic)*. Note that such a breach may also need to be reported under the *Notifiable Data Breaches Scheme* and/or the DHHS *Client Incident Management System* (CiMS).

Refer to Thorne Harbour Health *Notification of Privacy Breaches Work Instruction* for further details.

7. Communication

All Thorne Harbour Health employees, volunteers, members of the board and contractors will be informed about Thorne Harbour Health's *Privacy and Confidentiality Policy* and related procedures.

Clients will be informed about the Policy on intake and about their right to complain should a breach of their privacy occur. This information will be conveyed in printed form and verbally.

Thorne Harbour Health's *Privacy and Confidentiality Policy* and related procedures will be uploaded to the Thorne Harbour Health Intranet for easy access by employees, volunteers and the board. A *Privacy and Confidentiality Statement* summarising the *Privacy and Confidentiality Policy* will be available via Thorne Harbour Health's website for easy access by clients, members and community, other external stakeholders and other interested parties. Thorne Harbour Health's *Privacy and Confidentiality Policy* in full will also be available on request.

8. Review

The Thorne Harbour Health *Privacy and Confidentiality Policy* will be reviewed every three years after initial approval, or earlier if required. Circumstances that may prompt review include changes to relevant legislation; changes to Thorne Harbour Health's constitution; formal undertakings to work with other organisations; or organisational restructure.

Reviews will follow the procedures detailed in the *Development and Review of Policies, Procedures and Work Instructions Policy and Procedure*.

9. References

BNG MSO, *11.1.6 Privacy,* MSO Policy Template

BNG MSO, *11.1.7 Confidentiality,* MSO Policy Template

BNG MSO, *11.9.5 Client Records,* MSO Policy Template

BNG MSO, *11.11.4 Access to Confidential Information,* MSO Policy Template

Department of Health, *Privacy Policy*
http://www.health.vic.gov.au/privacy.htm

Department of Health and Human Services, *Reporting privacy breaches to the Department* (Fact sheet for funded organisations), September 2017
https://dhhs.vic.gov.au/search/results/privacy%20incident%20reports

Department of Health and Human Services, *Privacy incident report form*, November 2017
https://intranet.dhhs.vic.gov.au/privacy

Department of Human Services, *Privacy Policy*
http://www.dhs.vic.gov.au/about-the-department/documents-and-resources/policies,-guidelines-and-legislation/department-of-human-services-privacy-policy

Fair Work Ombudsman *Best Practice Guide Workplace Privacy* Commonwealth of Australia, 2014

Office of the Australian Information Commissioner, *Data breach preparation and response: A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)*, February 2018

https://www.oaic.gov.au/resources/agencies-and-organisations/guides/data-breach-preparation-and-response.pdf

Attachment 1: Summary of Privacy Principles

The table below provides a summary of the key privacy principles outlined in the *Health Records Act 2001,* the *Privacy and Data Protection Act 2014* (Victoria) and the *Privacy Act 1988* (Commonwealth). Full versions of these Principles are provided respectively in these Acts.

Summary - Health Privacy Principles (Vic) and Information Privacy Principles (Vic)	Summary - Australian Privacy Principles
1. Collection (HPP, IPP) ▪ Only collect health information if necessary for the performance of a function or activity and with consent (or if it falls within HPP1). Notify individuals about how the information is used and that they can gain access to it	**APP 3 – collection of solicited personal information** ▪ Only collect personal information that is necessary for your functions or activities ▪ Sensitive information about an individual must not be collected unless the individual consents to the collection of the information, and the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities ▪ If personal information is collected it must only be by lawful and fair means. **APP 5 - notification of the collection of personal information** ▪ At the time you collect personal information or as soon as practicable afterwards, take reasonable steps to make an individual aware of: ▪ why you are collecting information about them ▪ who else you might give it to and other specified matters ▪ If an individual asks, take reasonable steps to let them know, generally, what sort of personal information you hold, what purposes you hold it for and how you collect, use and disclose that information.
2. Use and disclosure (HPP, IPP) ▪ Only use or disclose health information for the primary purpose for which it was collected or a directly related secondary purpose the person would reasonably expect. Otherwise, consent is generally required.	**APP 6 - use or disclosure of personal information** ▪ If an organisation holds personal information about an individual that was collected for a particular purpose (the primary purpose), the organisation must not use or disclose the information for another purpose (the secondary purpose) unless: (a) the individual has consented to the use or disclosure of the information **APP 7- direct marketing** ▪ If an organisation holds personal information about an individual, the organisation must not use or

Summary - Health Privacy Principles (Vic) and Information Privacy Principles (Vic)	Summary - Australian Privacy Principles
	disclose the information for the purpose of direct marketing.
3. Data quality (HPP, IPP) ▪ Take reasonable steps to ensure health information held is accurate, complete, up-to-date and relevant to the functions performed.	**APP 10 - quality of personal information** ▪ An organisation must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity collects is accurate, up to date and complete. **APP 13 - correction of personal information**
4. Data security and retention (HPP, IPP) ▪ Safeguard the health information held against misuse, loss, unauthorised access and modification. Only destroy or delete health information in accordance with HPP4.	**APP 11- security of personal information** ▪ Take reasonable steps to protect the personal information you hold from misuse and loss and from unauthorised access, modification or disclosure. ▪ Take reasonable steps to destroy or permanently de-identify personal information you no longer need
5. Openness (HPP, IPP) ▪ Document clearly expressed policies on management of health information and provide the policies to anyone who asks.	**Australian Privacy Principle 1- open and transparent management of personal information** ▪ There should be open and transparent management of personal information. ▪ An organisation must have a clearly expressed and up to date policy (the APP privacy policy) about the management of personal information by the organisation. ▪ Have a short document that sets out clearly expressed policies on the way you manage personal information and make it available to anyone who asks for it. ▪ An organisation must take reasonable steps to implement practices, procedures and systems to ensure their functions or activities complies with the Australian Privacy Principles
6. Access and correction (HPP, IPP) ▪ Individuals have a right to seek access to health information held about them in the private sector, and to correct it if it is inaccurate, incomplete, misleading or not up-to-date. *	**Australian Privacy Principle 12 - access to personal information** ▪ An organisation holds personal information about an individual, it must, on request, give the individual access to their information.

Summary - Health Privacy Principles (Vic) and Information Privacy Principles (Vic)	Summary - Australian Privacy Principles
	▪ If an individual asks, you must give access to the personal information you hold about them unless particular circumstances apply that allow you to limit the extent to which you give access - these include emergency situations, specified business imperatives and law enforcement or other public interests
7. Identifiers (HPP, IPP) ▪ Only assign a number to identify a person if the assignment is reasonably necessary to carry out the functions efficiently.	
10. Anonymity (HPP, IPP) ▪ Give individuals the option of not identifying themselves when entering transactions with organisations where this is lawful and practicable.	**Australian Privacy Principle 2 - anonymity and pseudonymity** ▪ If it is lawful and practicable to do so, give people the option of interacting anonymously with you
11. Transborder data flows (HPP, IPP) ▪ Only transfer health information outside Victoria if the organisation receiving it is subject to laws substantially similar to the Victorian HPPs.	**Australian Privacy Principle 8 - cross-border disclosure of personal information**
12. Transfer/closure of practice health service provider (HPP) ▪ A health service provider whose business or practice is being sold, transferred or closed down, and will no longer be provide services must give notice of the transfer or closure to past service users.	
11. Making information available to another health service provider (HPP) ▪ A health service provider must make health information relating to an individual available to another health service provider if requested by the individual.	
12. Sensitive information (IPP) ▪ The privacy legislation restricts collection of sensitive information such as an individual's racial or ethnic origin, political views, religious beliefs, sexual preferences, membership of groups or criminal record.	

Sources: Department of Health and Human Services, *Privacy Policy*, http://www.health.vic.gov.au/privacy.htm visited 16/4/2015 (HPP and IPP); BNG NGO Services Online, *Info Sheet 7.29: Australian Privacy Principles*