Confidentiality & Privacy Policy

1. Purpose & Scope

This policy provides an outline of APMHA HealthCare Ltd. legal obligations and ethical expectations in relation to privacy and confidentiality and applies to all APMHA staff and consumers of APMHA services.

2. Policy

APMHA is committed to protecting the privacy and confidentiality of customers, consumers, and all other APMHA staff in the way information is collected, stored and used.

2.1. Collection

Collection of personal information must be fair, lawful, not intrusive and in alignment with APMHA's:

- Consumer Health Records Policy
- Client Privacy and Rights Charter
- Information Management Policy
- Open Disclosure Policy

A person must be told:

- The name of the organisation collecting
- The purpose of collection
- How the person can get access to their personal information
- What happens if required information is not distributed

APMHA will only collect personal information necessary to undertake our programs, activities or functions. Personal information about an individual will only be collected by lawful and fair means and directly from the individual wherever possible.

APMHA will ensure that each individual providing personal information is informed about and understands the purpose of collecting the information, to whom or under what circumstances their personal information may be disclosed to another party, and how they can access the information held about them by APMHA.

APMHA will collect commercial information that is already available in the public domain. This includes operating details of primary healthcare providers in the region. APMHA will seek to preserve the accuracy of this information.

2.2. Use and disclosure

APMHA only uses or discloses information for the purpose it was collected unless:

- The person has consented,
- The person is underage and requires carer involvement,
- The person is considered 'at risk' and requires carer involvement,

- The person has identified a carer to be involved in their recovery plan,
- The secondary purpose is related to the primary purpose and a person would reasonably expect such use,
- Disclosure or the use is for direct marketing in specified circumstances, or
- In circumstances related to public interest such as law enforcement and public or individual health and safety.

If information is to be used for a secondary or unrelated purpose, such as service evaluation, consent is not required as the data will be de-identified. Clients will be given the opportunity to refuse such use or disclosure. If an individual is physically or legally incapable of providing consent, a responsible person (as described under the Privacy Act 1988) may do so.

APMHA will only disclose personal information without consent where such disclosure is required by law, or for law enforcement, or in the interests of the individual's or the public's health and safety. APMHA will keep records of any such use and disclosure. Information may only be disclosed to a responsible person (as described under the Privacy Act 1988).

2.3. Information quality and security

APMHA takes reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up to date. APMHA takes steps to protect the personal information it holds against loss, unauthorised access, use, modification or disclosure and against other misuse.

All personal information held by APMHA will be:

- If in paper form, received and stored in a secure, lockable location,
- If in electronic form, password and firewall protected, and externally backed up with a provider contractually bound to confidentiality,
- Accessible by staff only on a "need to know" basis, and
- Not taken from the APMHA offices unless authorised and for a specified purpose.

APMHA destroys or permanently de-identifies personal information that is no longer required to be held by legislation and by the APMHA. If it is necessary for the personal information to be given to a person in connection with the provision of a service, everything reasonably within the power of APMHA is done to prevent unauthorised use or disclosure of personal information.

2.4. Maintaining confidentiality

All APMHA staff are required to protect client confidentiality and privacy by:

- only discussing clients in a private and soundproof place and only with the relevant people
- not using client's names
- avoiding downloading or printing client files, and do not remove client information from the office
- activating the secure screen saver when leaving your desk
- logging out of your Google account, Chrome and Client Management Systems at the end of day or when away from your desk for an extended period

- use a unique identifier when recording information about clients on a database
- offer the client an alternative entry or exit point to avoid the public waiting room if required
- remove identifying information when discussing cases for professional development or teaching purposes.

2.5. Openness

This policy will be made available to any person upon request.

A general statement describing APMHA approach to privacy is accessible to the public via the website (www.apmha.com.au).

This is also provided to clients at the commencement of treatment services, on APMHA's Client Consent and Transition Form and provided to all staff working in APMHA services through the relevant Service Delivery Manuals.

2.6. National Privacy Principle 6: Access and Correction

Individuals may request access to their own personal information. Access will be provided unless there is a sound reason under the Privacy Act 1988 or other relevant law to withhold access. Other situations in which access to information may be withheld may include when:

- There is a threat to the life or health of an individual,
- Access to information creates an unreasonable impact on the privacy of others,
- There are existing or anticipated legal dispute resolution proceedings, and
- Denial of access is required by legislation or law enforcement agencies.

APMHA responds to a request to access or amend information within 45 days of receiving the request.

Amendments may be made to personal information to ensure it is accurate, relevant, up to date, complete and not misleading, considering the purpose for which the information is collected and used. If the request to amend information does not meet these criteria, APMHA may refuse this request.

If the requested changes to personal information are not made, the individual may make a statement about the requested changes and the statement will be attached to the record. APMHA is responsible for responding to queries and requests for access and amendment to personal information.

2.7. Identifiers

It is the policy of APMHA, that an identifier assigned by a Commonwealth or State/ Territory government 'agency', for example Medicare or Veterans Affairs numbers, will not be used to identify personal information.

2.8. Anonymity

APMHA gives people the option to interact anonymously whenever it is lawful and practical to do so.

An individual who chooses to access the services of the APMHA anonymously will be advised of any potential consequences resulting from their decision (e.g. where the lack of a contact name or address may jeopardise care in an emergency situation).

APMHA will not automatically preclude an individual from participating in the activities of APMHA because they request anonymity.

2.9. Trans-border data flows

APMHA only transfers personal information about an individual to someone who is in a foreign country if:

- the individual consents to the transfer, or
- APMHA is reasonably sure that the information will not be held, used or disclosed inconsistently with the National Privacy Principles.

2.10. Sensitive information

APMHA considers all personal information as sensitive information and requires consent (written and verbal) to collect, store, use and/ or disclose this information. In other special specified circumstances relating to health services provision and individual or public health and safety, the consent process may vary. Information sharing for continuity of health care shall be with authorised individuals and organisations on a need to know basis and be directly relevant to the client's continuity of health care.

APMHA only collects sensitive information (as defined under the Privacy Act 1988) other than health information about an individual if:

- The individual consents, or
- The collection is required by law and is consistent with the provisions of National Privacy Principles.

2.11. Collection, use and disclosure of confidential information

Other information held by APMHA may be regarded as confidential, pertaining either to an individual or an organisation. The most important factor to consider when determining whether information is confidential, is whether the information can be accessed by the general public.

If staff are unsure whether information is sensitive or confidential to APMHA or its clients, general staff and stakeholders, staff must consult with direct line or relevant General Manager before transferring or providing information to an external source.

2.11.1. Organisational information

All APMHA staff agree to adhere to APMHA's Code of Conduct when commencing employment, involvement or a placement. The Code of Conduct outlines the responsibilities to the organisation related to the use of information obtained through their employment, involvement or placement.

2.11.2. Stakeholder information

APMHA works with a variety of stakeholders. The organisation may collect confidential or sensitive information about its stakeholders as part of a working relationship. APMHA staff are not permitted to disclose information about its stakeholders that is not already in the public domain without stakeholder consent. The manner in which employees manage stakeholder information will be clearly articulated in any contractual agreements that the organisation enters into with a third party and managed by the relevant General Manager.

2.11.3. Client information

Detailed information regarding the collection, use and disclosure of client information can be found in the *Consumer Health Records Policy* and associated procedures.

2.12. Breach of privacy or confidentiality

If a staff member of APMHA is dissatisfied with the conduct of a colleague regarding privacy and confidentiality of information, the matter should be raised with the employee's direct line manager/ relevant General Manager. If this is not possible or appropriate, follow the delegations indicated in the *Grievance Policy*. APMHA staff who are deemed to have breached privacy and confidentiality standards set out in this policy may be subject to disciplinary action.

If a client or stakeholder is dissatisfied with the conduct of an APMHA staff member, a complaint should be raised in accordance with APMHA's *Feedback, Complaints and Appeals Policy and Procedure.* Information about making a complaint is available to clients, stakeholders and can be found on APMHA website (www.apmha.com.au) and in client welcome information provided at the commencement of services.

3. Definitions

Privacy provisions: Privacy provisions of the Privacy Act 1988 govern the collection, protection and disclosure of personal information provided to APMHA HealthCare Ltd. by clients, contractors, General Managers and employees.

Confidentiality: Confidentiality applies to the relationship of confidence. Confidentiality ensures that information is accessible only to those authorised to have access and is protected throughout its lifecycle. Confidential information may be marked as such or deemed confidential by its nature; for example, it is information that is not available in the public domain.

Consent: Consent means voluntary agreement to some act, practice or purpose. Consent has two elements: knowledge of the matter agreed to, and voluntary agreement.

Organisational information: Organisational information includes publicly available, and some confidential, information about organisations. Organisational information is not covered in the Privacy Act 1988 but some organisational information may be deemed confidential.

Personal information: Personal information means information or an opinion (including information or an opinion forming part of a database) about an individual (Office of the Federal Privacy Commissioner, 2001). It may include information such as names, addresses, bank account details and health conditions. The use of personal information is guided by the Privacy Act 1988.

Public domain: The public domain in relation to confidentiality is "common knowledge"; that is, information that can be accessed by the general public.

4. Responsibilities

General Managers

The General Manager Operations is responsible for the development and implementation of the policies, procedures and other governance tools required to comply with organisational and statutory privacy requirements. This will include ongoing enforcement, monitoring and evaluation of APMHA

HealthCare Ltd.'s privacy processes. General Manager Clinical and General Manager Service Delivery may also be required to ensure correct implementation and application of the Privacy Policy.

APMHA Staff

Relates to APMHA employees, subcontractors and other staff acting on behalf of APMHA. Staff must:

- Be familiar with the legislative requirements regarding privacy and the collection, storage and use of personal information.
- Understand the organisation's ethical standards regarding the treatment of other confidential information relating to APMHA HealthCare Ltd., its clients, contractors, employees and stakeholders.
- Act in accordance with organisational systems in place to protect privacy and confidentiality.
- Comply with Privacy Policy, Procedure and associated governance instruments.