

## Privacy Policy

### Purpose

To outline a framework for Capital Health Network (CHN) to responsibly manage the information provided by individuals and organisations in accordance with Australian Privacy Principles (APP) which came into force on 12 March 2014.

### Scope

This policy applies wholly or in part to CHN Board, management, employees, contractors and suppliers.

### Responsibilities

The CEO is responsible for the effective implementation of this policy.

All Board members, management and staff are responsible for complying with this policy.

Staff are responsible for seeking a written exemption from the CEO in any situations where they are unable to follow this policy or its procedures.

### Definitions

Privacy Officer is the person appointed by the CEO to manage the CHN information privacy processes and requests for information or access to individual records.

The Privacy Officer for CHN is the Director Corporate Operations.

Consent is defined in the *Privacy Act 1988* as express consent or implied consent which has 4 key elements:

- the consent must be voluntary
- the individual must be adequately informed before giving consent
- the consent must be current and specific
- the individual must have the capacity to understand and communicate their consent.

Health Information means information or opinion about:

- the health or a disability (at any time) of an individual
- an individual's expressed wishes about the future provision of health services to them
- a health service provided, or to be provided, to an individual
- other personal information collected to provide a health service
- other personal information about an individual collected in connection with the donation or intended donation, by the individual, of his or her body parts, organs or bodily substances.

Individuals are: Board members; Members; employees; members of the public accessing CHN programs (including their guardians if the individual is a child under 18), services and/or website; suppliers/contractors; job applicants; referees.

Personal Information is defined by the Privacy Act as "information about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion" which is maintained electronically, on video or in written/printed form and/or verbal information given to an employee about an individual.

Sensitive Information means personal or health 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 preferences or practices
- criminal record.

### **Underlying Principles**

The following underlying principles establish the policy framework for all areas of activity within CHN:

1. CHN regards having the information of individuals as a privilege
2. Individual/organisations' access to information about them is a right
3. The collection and storage of unnecessary information about individuals is considered a breach in privacy and is inappropriate
4. The formation of or expression of a professional assessment/opinion must be recorded with care
5. All individuals have the right to be informed about whom has access to their information
6. Individuals have a right to challenge the accuracy of personal information recorded about them
7. Wherever it is lawful and practicable, individuals can have the option of not identifying themselves

### **Policy**

CHN acknowledges and respects the privacy of individuals and meets the requirements of the Australian Privacy Principles.

### **Collection of personal information**

CHN will make every effort to only collect information with the prior knowledge and consent of the individual. Where we collect information about an individual without their knowledge, we will take all reasonable and practical steps to inform the person that we have collected their information from someone or somewhere else.

At the time information is collected (or as soon as practicable after) individuals will be made aware of:

- the purpose for which the information is collected
- their right to make reasonable requests to access that information
- how to contact CHN
- the period of time for which the information is kept
- the organisations (or types of organisations) to which CHN usually discloses information of that kind
- any law that requires the particular information to be collected
- main consequences (if any) for the individual if they provide incomplete or inaccurate information.

### **Collection of sensitive information**

Sensitive information will only be recorded with the individual's consent unless:

- the collection is required by law
- the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual whom the information concerns:
  - a) is physically or legally incapable of giving consent to the collection
  - b) physically cannot communicate consent to the collection
- the collection is necessary for the establishment, exercise or defence of a legal claim.

### **Information CHN collects**

CHN collects and holds the following information about members and stakeholders on the Chilli database:

- |                    |                                  |
|--------------------|----------------------------------|
| • Name             | • Gender                         |
| • Address          | • Date of Birth (if provided)    |
| • Organisation     | • Class of membership            |
| • Telephone number | • Languages spoken (if provided) |
| • Fax number       | • Practice role                  |

- Mobile telephone number
- Business email address
- Personal email address (if provided)
- Provider number
- Privacy request
- Special interests
- Dietary requirements (if provided)
- CPD number

This information is collected in order for CHN to conduct its business of being a primary health care organisation which supports and services primary health care professionals, community organisations, health care consumer organisations and the ACT community.

CHN may collect and hold sensitive health information about individuals for inclusion on their electronic health record at Capital Health Network.

The information held on a client or organisation will be up-to-date, relevant, non-obtrusive and objective.

### **Option of anonymity and pseudonymity**

In circumstances where CHN will have no need to contact an individual in the future, and is not required or authorised by law to deal with identified individuals, they have the right to anonymity and/or the right to use a pseudonym when providing information.

Where an individual is receiving an ongoing health service, they have the right to receive those services either anonymously or by using a pseudonym. However, CHN will need a contact phone number in order to be able to contact or follow up with the individual.

Any person who chooses not to disclose their name or who uses a pseudonym will not be discriminated against nor refused clinical service because of their choice.

CHN is unable to extend membership to an individual who chooses to be anonymous or use a pseudonym.

### **Purpose of information collection**

CHN collects information about individual members and stakeholders in order to meet constitutional requirements, provide member services, provide support services and supply regular communication about CHN activities and events.

CHN collects sensitive health information about individuals who are clients of clinical programs in order to provide the clinical service for which they have been referred.

### **Access to and correction of information**

Individuals have the right to request access to information held by CHN about them. CHN will provide access to this information within 10 working days and any costs related to access to the information will be borne by CHN. Individuals can access their information by submitting a written request to:

Information Privacy Officer  
 Capital Health Network  
 PO Box 9  
 Deakin West ACT 2600

Requests must state:

- the name and address of the individual;
- sufficient information to identify the health record;
- the way in which the individual wishes to have access.

An individual may exercise their right of access to their information by having the record explained to them by a health service provider.

CHN will take all reasonable steps to be satisfied that the individual requesting access to information is the individual referred to in the information. This may include asking for photo identification and/or proof of guardianship.

If an individual believes that the information held by CHN is inaccurate or incomplete, CHN will take all reasonably practical steps to correct inaccurate, incomplete or out-of-date information. CHN will not delete information from health records but will make appropriate corrections or additions to the record.

### **Refusal to produce information**

CHN may refuse to provide access to health records if:

- the record relates to matters covered by reporting under the *Children and Young People Act 2008* or notification under the *Children's Services Act 1986*
- CHN believes the information in the record would constitute a significant risk to the individual or any other person if it was produced
- CHN believes that a health professional should discuss the record with the individual
- Parts of the record are confidential.

### **Disclosure of information**

CHN may disclose publicly available information about its members if CHN would regularly disclose such information or could reasonably be expected to disclose the information.

CHN will not disclose information about the health status of individuals receiving clinical services to anyone other than the individual without the consent of the individual.

### **Legal requirements to disclose information**

A legal requirement to disclose personal information may override this policy.

Situations where this may occur include:

- when the information is required to be provided under subpoena
- when serious criminal acts are known
- where there is serious risk of abuse or physical harm to the individual or other person including CHN's employees
- suspected abuse or neglect

In the event that a legal need for disclosure arises, the employee will inform and discuss the issue with their manager (where practicable) prior to making a decision to breach privacy.

### **Protection of information**

CHN will have processes and procedures in place to protect the information that CHN has under its control from:

- a) misuse, interference and loss
- b) unauthorised access, modification or disclosure.

### **Violation of an individual's privacy**

Deliberate violation of an individual's privacy by a member of staff will be considered gross misconduct and grounds for instant dismissal. Legal action may also be taken.

This includes accessing a staff person's personnel record, health record or performance review records unless authorised.

### **Staff access to individual's files**

Individuals' files are to be accessed only by staff members providing a service to that individual.

Files containing the personal information of individuals will not be taken from the CHN office unless authorised and for a specific purpose.

Information held by CHN about individuals will be stored securely whether in paper or electronic form.

Information held about individuals will be destroyed or permanently de-identified if it is no longer needed.

### **Third-party access to information**

Where contractors/suppliers who are performing a service for CHN have access to personal information (such as access to CHN's database or server) they will be required to sign a non-disclosure agreement prior to commencing their contract with CHN.

### **Commonwealth Government identifiers**

CHN does not use Commonwealth Government identifiers to identify any individual.

No staff member will disclose a Commonwealth Government identifier should they become aware of it.

### **Overseas transfer of information**

Where CHN transfers or stores personal information or data overseas, the following provisions will be in place:

- Individuals will be expressly informed that their information will be stored overseas
- Individuals will consent to their information being stored overseas
- The overseas recipient will handle the information in accordance with the APPs
- The overseas recipient will be subject to laws that provide similar or more stringent privacy protections
- CHN will have a binding contract with the overseas recipient that:
  - Personal information is handled according to the APP
  - The recipient complies with the APP in relation to collection, use, disclosure, storage, destruction and de-identification of personal information
  - Ensures a complaint handling process is in place
  - The recipient has a data breach response plan which includes notification of CHN should it be suspected that a breach has occurred.

These requirements are transferrable to any agency CHN provides data to as part of a contract or commissioning process.

### **Destruction of information**

CHN will remove information from records when it is no longer required. The treatment of CHN records and individual health records, their retention and destruction or archiving is governed by the Records Management Policy and Procedures.

### **Availability of this policy**

This policy will be made available to members, stakeholders and the general public through the CHN website.

Any individual may request a paper copy of this policy by phoning 6287 8099 or by writing to:

The Privacy Officer  
Capital Health Network  
PO Box 9  
Deakin West ACT 2600

Or by email to: [reception@capitalhn.com.au](mailto:reception@capitalhn.com.au)

### **Complaints**

Any complaint in relation to CHN's handling of personal information should be directed to the CEO. Unless the complaint can be dealt with immediately and to the satisfaction of both parties, the complainant will be asked to lodge their complaint in writing so that CHN can respond to them personally. Any complaint received will be addressed using the CHN Managing Complaints procedures.

If an individual believes their complaint has not been appropriately addressed by CHN, they will be referred to the Office of the Federal Privacy Commissioner Privacy Hotline on 1300 363 992.

**Legislation**

This policy is compliant with:

*Australian Privacy Principles;*

*Privacy Amendment (enhancing Privacy Protection) Act 2012*

*Privacy Act 1988*

*Health Records (Privacy and Access) Act ACT 1997*

**Review History:**