Information Privacy

Introduction

Information privacy is about empowering individuals to manage, as far as practicable, the collection, use and dissemination of personal information about themselves. It incorporates safeguards for a range of personal information handling activities such as collection, storage, access, transmission, disclosure, use, and disposal.

Policy

WATCH is committed to protecting the privacy of personal information which is requested and handled on behalf of the clients and staff. WATCH respects the right to privacy of individuals and any personal information provided by the clients and staff (including volunteers) to the organisation will be held in confidence.
This policy outlines how WATCH handles personal and health information in accordance with the Information Privacy Act 2000 and the Health Records Act 2001. The policy also applies to information about individuals obtained from other sources.

Collection of Information

WATCH collects and handles a range of personal information for the purposes of providing services or to carry out statutory functions. WATCH also collects some personal information for planning, funding, monitoring and evaluation of services and functions. However, where practicable, identifying details for these purposes will be removed. The information will otherwise be restricted to program use and organisational management, unless requested for legal purposes.

WATCH will only collect the information that is necessary to provide an efficient and appropriate service. Clients and staff will be advised if information relating to them is collected from other sources. Consent to use this information for any other purpose(s) will be requested from the individual.

WATCH endeavours to monitor all incoming electronic mail and to ensure personal information is stored securely once received. The data may be printed or saved in a document file. It is deleted from email thereafter. WATCH does not generally transmit personal data via email. However, where this is requested for legal purposes, a confidentiality statement will be attached to the outgoing data.

Use and Disclosure

There are very few situations when information will be shared without obtaining specific consent. For example, in an emergency situation without obtaining specific consent. For example, in an emergency situation we would need to release medical or personal information to aid emergency treatment. However, when WATCH updates clients' medication details periodically, carers are advised that releasing such information implies their consent to reveal it under emergency conditions.

Also in certain circumstances, this organisation may be required by law to release personal information. Examples include:

- Reporting notifiable diseases to the Department of Human Services.
- Providing health records to a court when required in relation to legal proceedings.
- Providing health records to a law enforcement agency in response to a search warrant.

If any of these circumstances apply, WATCH will advise the person as soon as possible that their information has been released and the purpose of its release, where appropriate.

Data Quality
WATCH endeavours to ensure that information held by the organisation about clients and staff is accurate and up-to-date. WATCH encourages individuals and carers to notify of any changes or inaccurate information so that it can be updated or corrected.

Data Security
At WATCH, every effort is made to ensure that personal data remains secure, protecting it from unauthorised access. Information or data is restricted to those who need to know and the distribution of such information is kept to a minimum.

Openness
WATCH is completely open with what is done with personal information. This is communicated by way of:

- This information privacy policy
- Privacy statements included on correspondence of a personal nature
- The information Privacy handout
- WATCH's website

Data Access and Correction
Clients, or their authorised representative, and staff may review any personal data about them held by WATCH by contacting the Program Manager or C.E.O... The person may request that any information be corrected.

Data Transfer
Other than for the purpose of Government Data Collection, WATCH does not transfer personal information outside the organisation. When legally required to do so, for example through *Freedom of Information Act,* information will be transferred by mail or fax that has a confidentiality statement attached. Clients and staff will be notified of this transfer as soon as practicable.

Sensitive Information
WATCH will not collect any sensitive information about clients and staff except where directed for a specific purpose.
Sensitive information is generally regarded as information relating to: ethnic background, religion, political viewpoints, sexual preferences and criminal records.

The requirements of the quarterly or annual State and Commonwealth Governments Statistical Data Collection include details of the ethnic background of our clients and their source of income. Other identifiers, such as names, phone numbers and addresses, are not used when supplying this information.

A mandatory requirement for employment with government funded organisations such as WATCH is a National Police Record Check. This applies equally to volunteers and others who are in regular contact with our clients, whether paid or unpaid.
The information supplied by the Police is placed in each staff member's personnel file and kept in a locked cabinet in the Office Manager's office.

No other sensitive information is retained by WATCH.

Disposal of Information
WATCH will retain personal information for the period authorised by the *Public Records Act 1973,* for seven years.

When a client leaves WATCH, their information is transferred by mail to the manager of their new service or held securely for the period indicated above and then shredded.

When a staff member leaves WATCH, their information is held securely for the period indicated above and then shredded.

WATCH has its own shredding machine and either the C.E.O. or the Office Manager carries out this shredding function. WATCH also uses a Private Shredding company, that collects material for shredding and gives a signed declaration that all work has been carried out according to legislation.

Archiving Process
After a period of two (2) years all client information regarding programs, assessments, and evaluations are stored in archive boxes which are placed in a locked room for a period of seven (7) years, after which these are shredded.

Breaches of this Policy
WATCH will ensure all staff, clients and members of the organisation are aware of the details contained in this policy and that personal information is kept in strict confidence and securely stored.

In the first instance, alleged breaches of privacy should be referred to the C.E.O. If a satisfactory resolution cannot be reached at this level, the alleged breach should be submitted to the Committee of Management.

If a person is not satisfied with the way in which WATCH handles their allegation and the breach remains unresolved, the Health Services Commissioner or the Victorian Privacy Commissioner may be contacted.

Responsibility
C.E.O., Managers and Supervisors

Procedure Owner
The C.O.M.