



Confidentiality and Privacy Policy

Policy: Confidentiality and Privacy	Area: Organisational	
Last Reviewed:	Board Endorsed: November 2015	Pages: 4

Rationale

To ensure that the highest standard of confidentiality is applied to all confidential information held at and by WACHS.

This policy is to be read in conjunction with the 'Confidentiality: Management of Personal Health Information' policy and procedure.

Evidence Base

This policy is consistent with the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*, the *Privacy and Personal Information Protection Act 1998* and the *Australian Privacy Principles*, as derived from the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*.

QIC 7th Edition: 2.3, 5.2.5

Definition

Personal Health Information is defined as information concerning a client's health, medical history, or past or present medical care; and which is in a form that enables or could enable the client to be identified.

It includes information about an individual's express wishes concerning current and future health services.

Related Documents

- Privacy, Confidentiality and Security Agreement
- *Privacy and Your Rights* brochure
- *Patient Information* brochure
- Confidentiality: Management of Personal Health Information policy and procedure.

Signing the Privacy, Confidentiality and Security Agreement

WACHS is committed to ensuring that the organisation complies with relevant privacy, confidentiality and security legislation to protect our clients, staff and our organisation. As part of this, individuals are required to understand their obligations and responsibilities including the contents are of this policy.

Definition

Confidential information is any information which has not been published and is not accessible to the general public. It includes information in any form including electronic or digital form.

With reference to this Service, confidential information includes, but is not limited to:

- **Personal Health Information**

WACHS collects personal health information for the purpose of providing services to clients. Please see the '*Confidentiality: Management of Personal Health Information*' policy and procedure.

It is to be noted that only that information which is required for the purpose of performing duties is to be accessed.

- **Personal Information Other Than Personal Health Information**

Any personal information acquired expressly or indirectly that relates to current or former employees, officers, directors, clients, volunteers, contractors, students or trainees.

- **Financial Information**

Any financial information whatsoever that is not published and accessible to the general public. It includes but is not limited to the financial information of the Service, current or former directors, officers, related bodies corporate, clients, employees, contractors, volunteers, students and trainees.

- **Commercial and Business Information**

Any information which is the information of WACHS and which has not been published for access by the general public. It includes but is not limited to third party arrangements such as contractual arrangements, operational matters and strategic and policy matters.

Security

Security is the security of WACHS and all of the property of WACHS, intellectual or any other property whatsoever.

With reference to WACHS, confidential information includes, but is not limited to:

- **Internet Security**

This includes but is not limited to computer passwords and logons.

No person is to divulge to any person whatsoever their password or logon.

It is expressly prohibited to access websites containing any pornographic materials. It is also expressly prohibited to access gambling sites.

- **E-mail Security**

This includes all incoming, outgoing and internal email. It is the policy of WACHS that no emails are to be accessed by, forwarded by or received by persons using the equipment of the Organisation that contain any pornographic material or any offensive material whatsoever including but not limited to offensive language, racial slurs, sexist slurs or any other material deemed by the Organisation to be offensive. No person is to forward internally or externally any emails that do not relate to the duties of the person sending the email.

Policies and Procedures

This Service has comprehensive policies and procedures related to privacy and confidentiality. The primary policy with respect to personal health information is 'Confidentiality: Management of Personal Health Information'.

It should be noted that many policies contain provisions for privacy and confidentiality, including all policies and procedures related to client consent and data storage and management.

Consequences of Breaches of Confidentiality

WACHS is bound by legislation relating to privacy and personal health information. It is also bound by the quality standards the organisation has set internally and which have been and continue to be, externally assessed by auditors.

Breaches of confidentiality may result in one or more of the following:

- Pain and suffering to the person whose confidentiality has been breached
- Disciplinary action
- Civil action against a person for breach and damages
- Criminal charges against an individual
- Criminal charges against the organisation
- Civil action against the organisation
- Sanctions imposed by the Privacy Commissioner
- Fines imposed by the Privacy Commissioner
- Loss of professional registration

Examples of Breaches

To assist in understanding the nature of breaches, some examples have been provided. These examples should not be considered as exhaustive in any way of the type of breach that may occur or may be deemed to have occurred.

1. **Accessing information that you do not need to know to do your job, for example:**

- Accessing information on family, friends or co-workers
- Reading client files without proper reason or authority
- Accessing without authority, employee or organisation information that is not specifically required for the performance of duties within the ambit of the person's duties

2. **Divulging personal information by, for example:**

- Conducting a conversation relating to client or staff information in a public place
- Telling a relative or friend information about the confidential information of a staff member
- Discussing confidential information in a public area such as a corridor or shopping mall
- Accessing without authority or divulging information contained in employee files
- Accessing without authority or divulging information in respect to any aspect of employee pays including superannuation details, salary sacrifice details, banking details or any other information whatsoever
- Accessing without authority or divulging any information whatsoever in respect to personal contact information that may have been provided to WACHS

3. **Divulging commercial or business information by, for example:**

- Accessing or divulging without proper authority information related to any contracts with third parties or funding bodies
- Accessing or divulging information related to the finances of WACHS

- Accessing or divulging information related to confidential policy, strategic or operational matters of WACHS
- 4. *Sharing, copying or changing information without proper authorisation by for example:***
- Making unauthorised changes to a client's record
 - Making unauthorised changes to an employee file
 - Copying and forwarding client, employee or WACHS information to a third party without having verbal or written consent from a person in a position to provide authority
- 5. *Sharing your password, by for example:***
- Telling another person your logon password
 - Providing an unauthorised person the access codes for employee files or client accounts
 - Using unauthorised shared passwords
- 6. *Using another person's password, for example:***
- Using another person's password to log in to the computer system
 - Unauthorised use of a password to access employee files or client accounts
- 7. *Leaving a secure information system (that is, a system that is password protected) unattended while logged on, by for example:***
- Being away from your desk (for example, lunch breaks) while you are logged into the computer system
 - Allowing a co-worker to use a secure system for which she does not have access after you have logged in
- 8. *Leaving any of the property of the Organisation in a non secure location or state, for example:***
- Leaving vehicles unlocked
 - Divulging information about the property of WACHS in such a way that WACHS's property is put at risk
 - Leaving the premises unattended and unsecured
 - Leaving equipment unsecured

Signing the Privacy, Confidentiality and Security Agreement

It is a condition of employment with this service that all staff and board members sign the Privacy, Confidentiality and Security Agreement prior to commencement of work. This Agreement will be provided to new employees, board members, casual employees and students, volunteers and any other person who may have access to confidential information either directly or indirectly. The signed agreement must be submitted on the first day of employment.

Privacy Officer

For the purpose of managing complaints about privacy made to external agencies, the CEO is the designated Privacy Officer.