Confidentiality – Management of Personal Health Information

Policy: Confidentiality – Management of Personal Health Information	**Area:** Organisational	
Last Reviewed:	**Board Endorsed:** November 2015	**Pages:** 7

Rationale

To ensure that the legal and ethical right to privacy and confidentiality of all clients, staff and the organisation is upheld and respected at all times.

Evidence Base

This policy is consistent with the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*, (the *RACGP Handbook for the Management of Health Information in Private Medical Practice*, 2002) and the *Australian Privacy Principles*, as derived from the *Privacy Amendment (Enhancing Privacy Protection) Act 2012.*

Definition

Personal information means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained from the information or opinion.

Sensitive information means:

a) Information or an opinion about an individual's:

(i) Racial or ethnic origin

(ii) Political opinions

(iii) Membership of a political association

(iv) Religious beliefs or affiliations

(v) Philosophical beliefs

(vi) Membership of a professional or trade association

(vii) Membership of a trade union

(viii) Sexual preferences or practices

(ix) Criminal record

That is also personal information

b) Health information about an individual

c) Genetic information about an individual that is not otherwise health information.

Related Documents

- Privacy, Confidentiality and Security Agreement
- *Privacy and Your Rights* brochure
- *Patient Information* brochure

Signing the Privacy, Confidentiality and Security Agreement

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

An example of indirect access may be where an electrician has been engaged to perform maintenance work in the reception area, behind the desk where medical records are stored. The electrician may see a fax or a patient record. This person has therefore had indirect access to personal health information and is bound by the same laws and policies as other WACHS staff.

It is important that a contractor such as the person described, sign a confidentiality agreement to protect the organisation and it's clients. A briefer version of the Agreement has been developed for contractors onsite for brief periods of time and who will have access only indirectly to personal health information. Other contractors such as accreditation auditors and data management system maintenance auditors will be required to sign the full Agreement.

Privacy

- All Health Service staff must ensure that clients can discuss issues relating to their health, and that the attending doctor, counsellor, nurse, Aboriginal health worker or other staff member with whom the client is communicating, can record relevant personal health information, in a setting that provides visual privacy and protects against any conversation being overheard by a third party.
- Staff should not enter a consultation room during a consultation without knocking.
- Staff, registrars and students cannot be present during a client consultation without the prior permission of the client.

Informing New Clients of the Privacy Policy

Doctors or program workers are to discuss the Service's privacy policy at the first visit of a client or when it is clear that the client is continuing with the Health Service.

Clients are to be offered, in the content of the 'Privacy and Your Rights' brochure, access to the full information sheet.

It is the responsibility of the Clinic Team Leader to ensure that the 'Privacy and Your Rights' brochure is available in the waiting room at all times and is kept with other health information and promotion brochures.

Clients May Use an Alias and Remain Anonymous

Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter.

This does not apply if, in relation to that matter:

(a) The APP entity is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves

(b) It is impracticable for the APP entity to deal with individuals who have not identified themselves or who have used a pseudonym.

Clients may access health services using an alias, as long as it is lawful and practical to do so. Some people may choose to use an alias for particular blood tests or pathology tests. This means that a person may use an alias if they choose to do so. An example of an unlawful use of an alias would be to knowingly use another person's name. This could be fraud. Clients will be encouraged to use a consistent alias or code to enable records to be kept for continuity of care. This means that client's who choose to use an alias should be encouraged to use the same alias and not change aliases.

If applicable, clients using an alias should be informed that the usual Medicare rebate may not be claimable and should this be the case, the client may be liable for payment equivalent to the claimable Medicare rebate.

Clients May Restrict Access to Their Personal Health Information

Where appropriate and necessary (that is where it has been requested by a client), doctors should provide an opportunity for clients to limit access to their record and will note any requirements in red ink in the front of the paper record or in the 'alert' section of the computerised record (for example specifying the name of a staff member that the client does not want to access their personal health information).

Doctors, Aboriginal health workers and nurses should make a note in the client's paper and electronic record outlining the client's consent to the collection and use of information that is particularly sensitive. This note is to be made at the time the client gives their consent, not at a later date.

How Information is Collected

Information is collected in 3 ways:

1. The patient provides information either at the time of making an appointment; at presentation to that appointment and during a consultation with the doctor, nurse of Aboriginal health worker.
2. Medical results received following a referral for specialist services (e.g. pathology).
3. Referral to WACHS from external source.

How Information is Stored

WACHS now uses an electronic medical records system titled "Communicare". This system allows for greater security around health records. Only staff with specific permission can access "Communicare" records.

Client Access to Their Personal Health Information

Under privacy legislation provisions clients may access their health information stored at the Health Service. This access is not to be unnecessarily obstructed and is to be as easy for the client as is practical. The treating doctor will provide an up to date and accurate summary of the client's health information on request or whenever appropriate. It is a matter for the treating doctor to determine if a request for access can be accommodated immediately the request is made, or if the client is to be asked to return at a later, more convenient time.

- The treating doctor will consider all requests made by a client for access to their medical record.
- In doing so the doctor will need to consider the risk of any physical or mental harm resulting from the disclosure of health information.
- In circumstances where the client does not have a treating doctor, or where the treating doctor is on leave, all requests are to be directed to the Clinic Team Leader.

- If the doctor is satisfied that the client may safely obtain the record they will show the client the record, and explain the contents to the client.
- Any information supplied by a third party, which may breach the privacy rights of the third party, or cause harm to the third party if disclosed, should be removed from the file prior to providing access. An example of this is where information about a client's mental health has been provided by a family member and that this has been recorded in the notes.
- Any information that is provided pursuant to child protection legislation is confidential and should be removed from the medical record before providing the information to the client. Reporters who report pursuant to child protection legislation are protected from disclosure of their identity.
- The client is entitled to a photocopy of their medical records subject to the above.
- This Health Service will respond to a client's request for access within fourteen (14) days of the request.

Correction of Client Records

- Staff may alter personal health information at the request of the client when the request for alteration is straightforward (e.g. amending an address or telephone number).
- All other requests for alteration of medical records must be directed to the doctor.
- When a client requests that their medical records be altered, the doctor will annotate the client's record to indicate the nature of the request and whether the doctor agrees with it.
- As per the *Privacy Amendment (enhancing Privacy Protection) Act 2012*, it is not permissible to alter such as to obliterate the original entry.

Professional Development, Quality Assurance and Improvement

- The 'Privacy and Your Rights' brochure informs clients that professional development, and quality assurance/improvement (QA) activities are undertaken from time to time, to improve individual and community health care and Health Service management.
- Where possible, identifying information will be removed from records when undertaking these activities.
- The health information is for the purpose of improving care and is used for internal purposes only and is not given or disclosed to anyone outside of the employment of WACHS, unless the person is involved in the particular professional development or Quality Improvement activity.
- This Health Service participates in Health Service accreditation, which assists it improve the quality of its services.
    - Health Service accreditation may involve the auditors, who visit the Health Service reviewing client records to ensure that appropriate standards are being met.
    - This Health Service will advise clients when accreditation is occurring by placing a notice in the waiting room prior to the survey visit occurring.
    - Clients will be given the opportunity to refuse accreditation surveyors access to their (the client's) personal health information.

Client Recall

- The 'Patient Information' brochure is to contain the following statement:

  "Recall and Reminders: We are committed to preventive and holistic care. We may issue you with a reminder notice from time to time offering you preventive health services appropriate to your care. If you do not want to be part of these reminder systems please inform the receptionist or your doctor".

- Clients are to be given the "Consent to Recall and Reminders Information Sheet" on request.
- Clients who have queries about the recall and reminder system are to be referred to their doctor for a full explanation.
- If the client states that they do not consent to enrolment in the routine recall system, it is the responsibility of the receptionist or the doctor (if the client tells the doctor) to enter 'NO' in the 'Consent to Reminders' section on the summary section (front page) of the medical records in red ink.
- In *Communicare* select the Clinical record, select the client and click Clinical Item type.
- This will automatically be saved to appear on the summary section of the client's record.

It is to be noted that ***the above applies to routine reminder systems and specifically does not refer to recall of a patient with a clinically significant test result.*** Please refer to the 'Managing clinically significant results and tests' for the procedure.

Research

No health and medical research is undertaken at this health service without the consent of the CEO and Executive Management Team.

If consent is obtained all research is to be consistent with the ethical guidelines set by the AH&MRC, current legislation relating to medical and health research and current ethical guidelines as deemed applicable by the Health Service.

Disclosure of De-identified Information

Clients of this Health Service are to be informed, via the 'Privacy and Your Rights' brochure that de-identified health information may be provided to third parties.

If a client withdraws their consent for this to occur the following procedures are to be taken:

- The doctor will make a note of this on the inside of the front cover of the client's medical record and;
- In the 'Alert' section on the summary page of the electronic records the following is to be recorded, "Do not provide de-identified health information to any third party without express consent".

Note: This section of the procedure applies to de-identified information and does not include identified information. Disclosure of identified information always requires consent (see below).

Disclosure of Confidential Health Information to Third Parties

- Doctors, Aboriginal health workers, nurses and other staff will ensure that personal health information is disclosed to third parties only where consent of the client has been obtained.
- Exceptions to this rule occur when the disclosure is necessary to manage a serious and imminent threat to the client's health or welfare, or is required by law.

- For example, a doctor should refer to relevant legislation and the maturity of a minor before deciding whether the client (in this case a minor) can make decisions about the use and disclosure of information independently (i.e. without the consent of a parent or guardian). For example, for the client to consent to treatment, the doctor must be satisfied that the client (a minor) is aware and able to understand the nature, consequences and risks of the proposed treatment.
- This client is then also able to make decisions on the use and disclosure of his or her health information.
- Health care workers should explain to clients the nature of any information about the client to be provided to other people, for example, in letters of referral to hospitals or specialists.
- The client consents to the provision of this information by agreeing to take the letter to the hospital or specialist, or by agreeing for the Health Service to send it. This is implied consent.
- The client may request and upon request, should be shown the contents of information to be disclosed to third parties, in circumstances consistent with the above guidelines.
- Doctors and staff should disclose to third parties only that information which is required to fulfil the needs of the client. These principles also apply to the personal information provided to a treating team (for example, a physiotherapist or consultant physician also involved in a person's care).
- The principles also apply where the information is transferred by other means, for example, via an intranet.
- Information classified by a client as restricted will not be disclosed to third parties without the express consent of the client.
- Staff should make a note at the time that permission is given.
- Information disclosed to Medicare or other health insurers should be limited to the minimum required to obtain insurance rebates.
- Information supplied in response to a court order should be limited to the matter under consideration by the court.
- From time to time General Practitioners will provide their medical defence organisation or insurer with information in order to meet their insurance obligations.

Disclosure of Health Information for the Purpose of Shared care and Case Conferencing

Case conferencing and shared care is an important part of the holistic care offered by the Wellington Aboriginal Corporation Health Service. The service encourages clients to participate in this extended care by consenting to disclosure to team members. In this context, team members refers to team members external to WACHS. The same principle of consent applies to this as to other disclosures. The client's consent is to be obtained before health information is disclosed to third parties including employees of NSW Health. Consent may be verbal and is to be documented in the client's medical records in the same way as for other consents.

Requests for Personal Health Information and Medical Records by Other Medical Health Services

- If a client transfers away from the health Service to another health service and the client requests that the medical record be transferred, the treating doctor will provide the record, a summary, or a photocopy to the new health service or to the client.

- WACHS will retain original documents and records.
- Written permission for the release of the information must be obtained from the client prior to releasing the information.
- Any other request for personal health information from other health care providers must be treated in the same way as for any other release of information, that is, it must be with client consent.

Security

Staff and contractors must protect personal health information against unauthorised access, modification or disclosure and misuse and loss while it is being stored or actively used for continued management of the client's health care.

- Staff are to ensure that clients, visitors and other staff not required to have access, do not have unauthorised access to the medical record storage area or computers.
- Staff are to ensure that records, pathology test results, and any other papers or electronic devices containing personal health information are not left where they may be accessed by unauthorised persons.
- Non clinical staff should limit their access to personal health information to the minimum necessary for the performance of their duties.
- Fax, e-mail and telephone messages will be treated with security equal to that applying to medical records.
- Computer screens should be positioned to prevent unauthorised viewing of personal health information.
- Through the use of password-protected screensavers, staff are to ensure that computers left unattended cannot be accessed by unauthorised persons.
- All staff should ensure that personal health information held in the Health Service is secured against loss or alteration of data. This includes adherence to national encryption protocols.
- Client records must not be removed from the Health Service, except when required by clinical staff for direct client care purposes.
- Records will be kept securely while away from the Health Service and the responsible clinician will ensure that records are returned to the Health Service and left in an appropriate place for filing.
- Paper medical records and other papers containing personal health information should be filed promptly after each client contact at the soonest possible time but at least by the end of each day.
- Staff should ensure that manual and electronic records, computers, other electronic devices and filing areas are secured at the end of each day and that the building is locked when leaving.
- The data on the computer system is backed up daily and stored off site. This will be the responsibility of the IT officer.
- Backups should be routinely tested to ensure daily duplication processes are valid and retrievable. This will be the responsibility of the IT officer.

Complaints About Privacy Related Matters

Complaints in respect to privacy are to be dealt with as per the 'Managing Complaints' policy found in the Policies and Procedures Manual.

Retention of Medical Records

It is the policy of this service that individual client medical records be retained until the client has reached the age of 25 or for a minimum of seven (7) years from the time of last contact, whichever is the longer.

No record should be destroyed at any time without the permission of the treating doctor and the senior medical officer.

Staff Training

- Training of new staff members should include education on this policy.
- Ongoing education of staff should include education on this policy.

Updating This Policy

- It is the responsibility of the CEO to alert managers, Aboriginal health workers and any other relevant staff of any changes to the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*.
- It will be the responsibility of the CEO to ensure that any changes are reflected in this policy and that the 'Privacy and Your Rights' brochure is updated as required.
- Any changes are to be authorised by the CEO.
- Please refer to the automated 'Checking Legislative Changes' form for instructions on how to automatically receive legislative updates.

Privacy Officer

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

Documentation

Any breach of this policy, whether accidental or intentional should be reported by completing an accident/incident/near miss form and should be reviewed for the purposes of acting to rectify the particular breach or to minimise damage caused by the breach and for the purpose of reviewing processes to ensure ongoing Quality Improvement.