



CONFIDENTIALITY and PRIVACY POLICY

RATIONALE

To ensure that the privacy and confidentiality of all clients, staff, Board of Directors (BOD), volunteers and students at Katungul is upheld and respected at all times.

POLICY

All information provided that relates to a client, staff, director, volunteers and students is given in confidence and must be kept private. Katungul strives to create a private and confidential environment for all. Failure to comply with the Confidentiality and Privacy Policy may lead to disciplinary action being taken.

DEFINITIONS

Confidential information is any personal or health information or opinion, whether true or not, acquired directly or indirectly about an individual whose identity is apparent, or can reasonably be ascertained from the opinion or information. It includes information about Katungul which has not been published and is not accessible to the general public. It includes information in any form including electronic or digital form.

Information is given in confidence to Katungul and its employees by various people including clients and staff, community members, key stakeholders and business associates. The information is **private information** and must be dealt with in a way that is consistent with the *Privacy Act 1988 (Cwth)*.

With reference to Katungul, private information includes, but is not limited to:

- Personal Health Information: Katungul collects personal health information for the primary purpose of providing health care and other services to clients.
- Personal Information Other Than Personal Health Information: Personal information or opinion, whether true or not, acquired directly or indirectly about an individual whose identity is apparent, or can reasonably be ascertained from the opinion or information.
- 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 Katungul, current or former directors, officers, related bodies corporate, business associates, clients, employees, contractors, volunteers, students and trainees.
- Commercial and Business Information: Any information which is the information of Katungul 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 and negotiations, operational matters and strategic and policy matters.



POLICY

1. Agreement to Comply with Staff Confidentiality; Staff Code of Conduct; and Katungul Policy and Procedures

It is a condition of employment with Katungul that all staff have read and fully understand and then sign the [Agreement to Comply with Katungul Policy and Procedures](#) including reference to this policy prior to or upon commencement of employment. This Agreement will be provided to new employees, casual employees, students, directors and volunteers and any other person who may have access to Katungul information either directly or indirectly. The signed agreement must be submitted on the first day of employment/appointment.

2. Management of Information Internally

All information provided to Katungul that relates to a client is given in confidence and must be kept private.

- All Katungul staff must ensure that clients can discuss issues relating to them, and that the attending doctor, counsellor, nurse, Aboriginal Health Worker, caseworker or other staff member with whom the client is communicating, can record relevant personal information, in a setting that provides visual privacy and protects against any conversation being overheard by a third party.
- Staff shall not disclose the personal information of clients to any unauthorised person.
- An unauthorised person is a person that does not require the information for the purpose of performing their duties.
- Staff should not enter a consultation room during a consultation without knocking.
- Staff, registrars, students and volunteers cannot be present during a client consultation without the prior permission of the client.

2.1 Disclosure of Personal Information

Disclosure of personal information is not permitted unless the person provides their consent, or an exception applies under the National Privacy Principles.

Staff shall not disclose personal information to any third party unless:

- The person has given their consent
- The disclosure is required by law
- The disclosure is directly related to the primary purpose of collection. This means that the disclosure is for administrative purposes, for example, for the purpose of billing Medicare; or for another directly related secondary purpose.
- It is for quality improvement purposes relating to an audit, however not for staff training unless the information is de-identified
- There is a *serious and imminent* threat to an individual's life, health or safety
- The disclosure is necessary as part of an investigation, for example, pursuant to a medico legal claim



- Doctors, Aboriginal Health Workers, nurses, caseworkers and other staff will ensure that personal information is disclosed to third parties only where consent of the client has been obtained or another exception applies.
- Katungul staff 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 Katungul to send it. This is implied consent.
Note: If the referral is to be sent electronically, there is NO implied consent, the health care worker must obtain the client's verbal consent to forward the referral.
- The client may request and 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 primary purpose needs of the client. These principles also apply to the personal information provided to a treating team (for example, a physiotherapist or consultant physician involved in a person's care).
- The principles apply where the information is transferred by other means, for example, via an intranet.
- Staff should make a note in the client records at the time that consent 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 scope of the documents requested.

2.2 Disclosure of health information for the purpose of shared care and case conferencing

Client consent is required.

At times, case conferencing and shared care is used to optimise the holistic care of clients. Katungul encourages clients to participate in this extended care by consenting to disclosure to team members. In this context, team members refer to team members external and internal to Katungul. The same principle of consent applies to this as to other disclosures. The client's consent is to be obtained before 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, however in these circumstances, written consent is preferred.

2.3 Requests for personal health information and medical records by other medical health services

Client consent is required and will be required in writing, signed by the client.

- If a client transfers from Katungul 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.
- Katungul 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.

2.4 Informing new clients' of the Confidentiality and Privacy Policy

The overriding principle is that Katungul is open and transparent about:

- What information is collected
- Why it is collected
- How it is used
- How and when it is disclosed
- How it is protected
- How concerns or complaints about privacy are managed

Katungul staff are to discuss the Confidentiality and Privacy Policy at the first visit of a client or when it is clear that the client is continuing with Katungul. Clients are to be offered, in the content of the Client Information Privacy Policy (attached) access to this information. It is the responsibility of the Administration Officer to ensure that the Client Information Privacy Policy and associated information brochure is available in the waiting room at all times and is kept with other health information and promotion brochures.

2.5 Clients may use an alias

The principle is that people should be provided access to health care and that may mean they do not want to disclose their identity.

Clients may access Katungul 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. Clients will be encouraged to use a consistent alias or code to enable records to be kept for continuity of care.

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.

2.6 Clients may restrict access to their personal health information

Where appropriate and necessary, Katungul will provide an opportunity for clients to limit access to their record and will note any requirements in **Red (bold)** in the front of the paper or electronic record of the computerised record if applicable. If there is a breach of this access then the person responsible for the breach will be provided with a warning in writing and will risk dismissal should this occur a second time.



2.7 Client access to their personal health information

Under privacy legislation provisions, clients may access the information stored at Katungul. This access is not to be unnecessarily obstructed and is to be as easy for the client as is practical.

Katungul staff 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 staff member 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 practitioner will consider all requests made by a client for access to their health record.
- In doing so the practitioner will need to consider the overriding principle and obligation under the Privacy Act that clients may have access to their personal health information. Consideration must then be made of 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 practitioner or where the treating practitioner is on leave all requests are to be directed to the Senior Medical Officer, Community Work Advisor or the Branch Manager which ever is most relevant.
- 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. *E.g. 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 that would identify a reporter pursuant to child protection legislation is confidential and should be removed from the client record before providing the information to the client. Reporters who report pursuant to child protection legislation are protected from disclosure of their identity.
- If the practitioner is satisfied that the client may safely obtain the record they will show the client the record, and explain the contents to the client.
- The client is entitled to a photocopy or printed copy of their records subject to the above.
- Katungul will respond to a client's request for access within fourteen (14) days of the request.

2.8 Alteration of client records

- Staff may alter personal 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 records must be directed to the client's primary worker.
- When a client requests that their records be altered, the staff member will annotate the client's record to indicate the nature of the request and whether they agree with it.
- As per the *Privacy Act 1988*, it is not permissible to alter such as to obliterate the original entry.



3. Professional Development

- The Client Information Policy brochure informs clients that quality assurance/improvement (CQI) activities are undertaken from time to time, to improve individual and Community Service Management.
- Where possible, identifying information will be removed from records when undertaking these activities.
- Personal information cannot be used for education purposes unless it has been de-identified or the client has provided consent.
- The information is for the purpose of improving care and is used for internal purposes only and is not given or disclosed to anyone within or outside of the employment of Katungul without prior consent.
- Katungul participates in Continuous Quality Improvement (CQI), which assists to 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.
 - Katungul will advise clients when accreditation is occurring by placing a notice in the waiting room prior to the audit visit occurring.
- Clients will be given the opportunity to refuse accreditation surveyors access to their personal information.

3.1 Staff Training

- Training of new staff members should include education on this policy.
- Ongoing education of staff should include education on this policy.
- All staff must receive annual education and training on confidentiality of personal information.

4. Client Recall and Reminder System

- 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 practitioner".
- Clients are to be given the 'Recall and Reminder Information Sheet' on request.
- Clients who have queries about the recall and reminder system are to be referred to their Primary Worker 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 Primary Worker to enter 'NO' in the 'Consent to Reminders' section on the summary section (front page) of the medical records in **red and Bold**

It is to be noted that ***the above applies to routine reminder systems specifically.***



5. Research

No health and medical research is undertaken at this service without the written consent of the Katungul Board of Directors.

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

6. Disclosure of de-identified information

Clients of Katungul are to be informed, via the 'Client Information Privacy brochure that de-identified 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 practitioner will make a note of this on the inside of the front cover of the client's health record; and,
- In **RED Bold in the 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.

7. Security

Staff must protect personal information against unauthorised access, modification or disclosure and misuse and loss while it is being stored by Katungul.

- Staff are to ensure that clients, visitors and other staff not required to have access, do not have unauthorised access to the record storage area or computers.
- Staff are to ensure that records, pathology test results, and any other papers or electronic devices containing personal information are not left where they may be accessed by unauthorised persons.
- Non clinical staff should limit their access to personal 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 health records.
- Computer screens should be positioned to prevent unauthorised viewing of personal 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 information held by Katungul is secured against loss or alteration of data. This includes adherence to national encryption protocols.
- Client records must not be removed from Katungul. If a home visit is to be conducted, the necessary information only is to be taken to perform the home visit and the records are to be returned to the service as soon as the home visit is complete. If the record is not required for the home visit it should not be taken.



- Paper records and other papers containing personal information should be filed promptly after each client contact at the earliest 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 Branch Managers and the CEO.
- Backups should be routinely tested to ensure daily duplication processes are valid and retrievable. This will be the responsibility of the Branch Managers and the CEO.

8. Unauthorised use of Information about Family or Friends

Katungul employees should not use information about family or friends. This includes viewing records.

- If a close family member attends the service, wherever practical, all staff should request that another, unrelated staff member manage the client. An example of where this may not be possible is when there is only one receptionist on the desk and a family member attends for an appointment. In these circumstances it will be necessary for the receptionist to complete the necessary documentation usually required.
- The exception is where the client provides express consent for the family member to be involved with care; however this will require the written approval of the Branch Manager.
- It is prohibited for staff to access information about other staff, BOD or clients unless they are required to do as part of their position. Where this is the case, only that information which is required to perform the task is to be accessed and the information is not to be used or disclosed for any other purpose.
- Staff have a responsibility to notify their Branch Manager if a family member is seeking treatment or services from them. This is in order to protect the client, the staff member and Katungul.

9. Audits

From time to time Katungul conducts audits on client data access. The audits are random.

The audits provide the following information:

- a) The name of files accessed
- b) The level of access (for example whether the access was to the personal details page of a client file or whether health records were accessed)
- c) The name of the person who accessed the files
- d) The date of access
- e) The time of access
- f) The length of time the file was open for

Any suspicious activity is reported to the Branch Manager/HR Manager or CEO and an investigation is



conducted. The investigation will always include an interview with the person who accessed the records to determine if the access was authorised. Authorised means, directly related to the tasks required of the employee.

10. Consequence of Breaches of Privacy

Katungul is bound by legislation relating to privacy and personal health information including Breach provisions of the Commonwealth Privacy Act. It is also bound by the quality standards Katungul 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 privacy 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.
- Loss of employment.



Client Information Privacy Policy

Introduction

This privacy policy is to provide information to you, our client, on how your personal information (which includes your health information) is collected and used within our service, and the circumstances in which we may share it with third parties.

Why and when your consent is necessary

When you register as a client of our service, you provide consent for our staff and service staff to access and use your personal information so they can provide you with the best possible care. Only staff who need to see your personal information will have access to it. If we need to use your information for anything else, we will seek additional consent from you to do this.

Why do we collect, use, hold and share your personal information?

Our service will need to collect your personal information to provide healthcare and other services to you. Our main purpose for collecting, using, holding and sharing your personal information is to manage your health and wellbeing. We also use it for directly related business activities, such as financial claims and payments, service audits and accreditation, and business processes (eg staff training).

What personal information do we collect?

The information we will collect about you includes your:

- names, date of birth, addresses, contact details
- medical information including medical history, medications, allergies, adverse events, immunisations, social history, family history and risk factors
- Medicare number (where available) for identification and claiming purposes
- healthcare identifiers
- health fund details.

Dealing with us anonymously

You have the right to deal with us anonymously or under a pseudonym unless it is impracticable for us to do so or unless we are required or authorised by law to only deal with identified individuals.



How do we collect your personal information?

Our service may collect your personal information in several different ways.

1. When you make your first appointment our staff will collect your personal and demographic information via your registration.
2. During the course of providing medical or other services, we may collect further personal information.
3. We may also collect your personal information when you send us an email or SMS, telephone us, or communicate with us using social media.
4. In some circumstances personal information may also be collected from other sources. Often this is because it is not practical or reasonable to collect it from you directly. This may include information from:
 - your guardian or responsible person (where applicable)
 - other involved healthcare providers, such as specialists, allied health professionals, hospitals, community health services and pathology and diagnostic imaging services
 - you're health fund, Medicare, or the Department of Veterans' Affairs (as necessary).

When, why and with whom do we share your personal information?

We sometimes share your personal information:

- with third parties who work with our service for business purposes, such as accreditation agencies or information technology providers – these third parties are required to comply with APPs and this policy
- with other healthcare providers
- when it is required or authorised by law (eg court subpoenas)
- when it is necessary to lessen or prevent a serious threat to a client's life, health or safety or public health or safety, or it is impractical to obtain the client's consent
- to assist in locating a missing person
- to establish, exercise or defend an equitable claim
- for the purpose of confidential dispute resolution process
- when there is a statutory requirement to share certain personal information (eg some diseases require mandatory notification)
- during the course of providing medical services, through eTP, My Health Record (eg via



Shared Health Summary, Event Summary).

Only people who need to access your information will be able to do so. Other than in the course of providing medical services or as otherwise described in this policy, our service will not share personal information with any third party without your consent.

We will not share your personal information with anyone outside Australia (unless under exceptional circumstances that are permitted by law) without your consent.

Our service will not use your personal information for marketing any of our goods or services directly to you without your express consent. If you do consent, you may opt out of direct marketing at any time by notifying our service in writing.

How do we store and protect your personal information?

Your information may be held in a variety of ways within Katungul. Most commonly, your information may be held as a paper health record, and/ or an electronic health record forming part of a secure computerised database. Some information may also be held in the form of an image including x-ray or photograph, or as an audio or video recording.

We follow strict rules and policies regarding the secure storage of information in all formats in order to protect your information from unauthorised access, loss or other misuse.

Our service stores all personal information securely.

How can you access and correct your personal information at our service?

You have the right to request access to, and correction of, your personal information.

Our service acknowledges clients may request access to their medical records. We require you to put this request in writing and our service will respond within a reasonable time

Our service will take reasonable steps to correct your personal information where the information is not accurate or up to date. From time to time, we will ask you to verify that your personal information held by our service is correct and current. You may also request that we correct or update your information, and you should make such requests in writing to the Clinic Manager.

How can you lodge a privacy-related complaint, and how will the complaint be handled at our service?

We take complaints and concerns regarding privacy seriously. You should express any privacy concerns you may have in writing. We will then attempt to resolve it in accordance with our resolution procedure.



Written complaints should be addressed to the Chief Executive Officer, Katungul ACRH&CS, 26 Princes Highway Narooma , 2546.

You may also contact the Office of the Australian Information Commissioner (OAIC). Generally, the OAIC will require you to give them time to respond before they will investigate. For further information visit www.oaic.gov.au or call the OAIC on 1300 363 992.