



Qutekcak Native Tribe Confidentiality Policy and Procedure

Personal responsibility and communication guidelines

All staff, contractors and other personnel employed by Qutekcak Native Tribe (QNT) are required to treat **all** client information with the utmost confidentiality. Staff with access to confidential, private or sensitive information **is not** to divulge this information with any other personnel unless authorized to do so. If you are ever asked to divulge confidential information about a client by a person who has no authority to request this, please report the matter to your supervisor immediately. If you ever hear a Qutekcak Native Tribe (QNT) employee discussing information of a confidential and/or private nature in an inappropriate way (eg, chatting to a colleague in the office or telling friends in a social setting), you must report the matter to your supervisor immediately.

The easiest way to follow this policy is to remember one simple rule: **NEVER give out confidential and/or private information about a client** unless it's to an authorized person. (Authorized in Writing) This means not even to family members - we have no way of knowing a person's family situation, and that person has the right to withhold private information from his/her family members.

QNT takes the confidentiality and privacy of our clients very seriously, and will not hesitate to take disciplinary action against any employees that are in breach of this policy.

Ramifications of breeches of the confidentiality of records

In a health setting a client can take legal action against the staff member responsible under the Law of Negligence. Qutekcak Native Tribe (QNT) owes a duty of care to the client to prevent any "damage" to the client.

To avoid potential litigation by the client, Qutekcak Native Tribe (QNT) needs to prove that they have steps in place to prevent such a breach taking place. These are:

- Recruitment and selection of staff, incorporating police checks.
- Induction training of new staff on confidentiality and privacy and record keeping policy and procedures.
- Yearly staff training, reinforcing confidential Care Coordination policies and informing staff of any changes to policies.
- Correct audited procedures for record keeping.
- Security systems in place to monitor and record computer access to information.
- Security systems in place to regulate level of access to information for different staff.
- The police are called in if there appears to be any breach.

If the Qutekcak Native Tribe (QNT) policy and procedure regarding confidentiality of client information is not followed, the individual staff member (or staff members) will be responsible rather than QNT.

ALL staff at Qutekcak Native Tribe (QNT) is required to sign a confidentiality agreement when they begin employment. This is a legally binding document that clearly states your obligation to treat all client information in a confidential manner.

Personal information:

- Privacy of the individual's details must be maintained at all times.
- Personal information that needs to remain confidential includes the age, gender, address, and date of birth of the individual.
- Other topics that also need to remain private are details of health issues, family information. Any other information of a personal or sensitive nature should be discussed only with the appropriate people when and where others will not overhear the conversation.
- Staff should never discuss details of a person outside the confines of the QNT CC office. i.e.: in a local store or other establishment; this is a policy breach.

<http://www.westone.wa.gov.au/toolbox7/health/shared/resources/manual/confidentiality.htm> -
[top](#)

Access to records:

Records may be paper or computer based, stored on discs or CDs. Records have legal, administrative and cultural constraints on their storage and disposal.

- Staff do not all require the same level of access to information. The level of access required is determined by the person's job role.

- Security passes may be issued whilst the staff member is working on a particular job, and then withdrawn if the level of access required changes.
- Staff will require ID access or an electronic door pass to access data.
- Computer access is monitored and restricted to ensure that client confidentiality is maintained.
- Documents need to remain private and confidential, and must **at all times** be stored in a securely locked fire proof cabinet for access by authorized personnel only. Keys will be kept by the Care Coordination Program Administrator and not be available to Care Coordination staff.
- Documents are not to be left where members of the general public may access them as the information within them could be taken out of context or made public.
- Check with the provider prior to allowing family members to access documents. There may be information that the client does not wish their family, friends or others to know.
- Under the Privacy Act, clients are able to access their own health information.

Inter-organizational access

Records **may not** be transferred from one organization to another without management approval. Not all organizations have reciprocal privacy agreements, so care needs to be taken and the correct channels followed to ensure that any sensitive or confidential information is not passed over to someone that may not treat the information in the same confidential manner as your organization.

Computer and Internet confidentiality

- Within the organization there will be information that is sensitive and confidential in nature stored on the computer network.
- At no time is staff to allow access for visitors to view computer-based information. Information that is printed out must be filed in the appropriate place according to the department's protocols.
- Any information that is to be discarded must be placed into bins for shredding prior to being discarded.
- QNT has a confidentiality agreement that employees sign when they first join our staff. These agreements protect the privacy of clients by ensuring that all staff will not pass on information of a personal or sensitive nature to any outside source.
- All staff is issued with a number/code that gives them access to a particular level of computer access.

Release of information:

Telephone

- The only time transfer of information is appropriate over the telephone is between authorized personnel such as medical staff, supervisors and management. Authorized personnel will give their ID details to verify their identity.

- When answering the phone, never give out any information - refer the enquiry immediately to a supervisor, manager or member of medical staff.
- If you are ever in any doubt as to the caller's identity, or suspect that something is not right, inform a supervisor immediately and do not comply with any requests from the caller.

Press and media requests

- Never give information to the press or media. There is always a spokesperson for the organization that will be designated as the person to speak with them.
- Politely decline any requests and refer the person to a supervisor.

Storage of records

1. Records must be correctly stored and eventually destroyed (in line with legal requirements) by authorized personnel to make sure that information of a sensitive nature is not made public.
2. All records must be stored in a secure, safe area where there is no possibility of damage by pests, vermin or environmental factors.
3. Records will be stored in an internal organizational storage area.
4. The area will be safeguarded by security, with building access determined by an ID system to prevent access by individuals that do not have clearance.
5. When stored, there is a system for location of records to allow for ease of access by authorized staff.
6. Records will be transported in a safe and confidential manner ensuring that access is only given to authorized staff.

Locked bins

- Any confidential or sensitive paperwork is placed in locked bins and shredded prior to being sent for recycling.
- Records are kept for as long as they have value, which in the case of health records varies. It is generally for 10 years after the client's death, but can vary for certain conditions and cultural considerations.