Privacy Policy and Procedure

Purpose

Aboriginal and Torres Strait Islander Community Health Service Brisbane (ATSICHS) Brisbane is committed to ensuring the privacy and confidentiality of all personal information collected in the course of delivering health services, in accordance with the Australian Privacy Principles. The purpose of this policy is to communicate how ATSICHS Brisbane collects and manages personal information. It also seeks to ensure that ATSICHS Brisbane staff maintain patient privacy and confidentiality at all times and understand their obligations under the relevant laws.

Scope

All staff of ATSICHS Brisbane are required to work within the principles and work practices outlined in this policy.

Definitions

Consent means 'express consent or implied consent'. The four key elements of consent are:

- the individual is adequately informed before giving consent
- the individual gives consent voluntarily
- the consent is current and specific, and
- the individual has the capacity to understand and communicate their consent (APP Guidelines).

Personal Information means 'includes information that could be used to identify an individual'. The opinion of what personal information is subjected to controversy based on opinions, beliefs and perspectives.

Sensitive Information means 'personal information' that includes, but is not limited to:

- racial or ethnic origin
- political opinions or associations
- religious or philosophical beliefs
- trade union membership or associations

- sexual orientation or practices
- criminal record
- health or genetic information
- some aspects of biometric information.

Health Information means 'personal information about an individual's health, this may include information and opinions about illnesses, injuries and/or disabilities'. This includes but is not limited to:

- notes of symptoms or diagnosis
- information about a health service an individual has received
- specialist reports and test results
- prescriptions and other pharmaceutical purchases
- dental records
- genetic information
- wishes about further health services
- wishes about potential organ donation/s
- appointment and billing details
- any other personal information collected when a health service is provided

Records and/or Information means 'documents, databases or pictorial references that contain personal information, and other information that can be used to identify an individual. These are usually collected, received and maintained as evidence'.

Applicant means 'an individual that requests records and/or information'.

Court/Tribunal Order means 'an order, direction or other instruments made by:

- a court
- a tribunal
- a judge
- a magistrate

- a person acting as a judge or magistrate
- a judge or magistrate acting in a personal capacity
- and a member or an officer of a tribunal (s6(1))'.

Primary Guardian Parent means 'a parent or an individual who is primarily and legally responsible for a child's care and wellbeing', at the time the request for records and/or information is made.

Exempt Document means 'a document that is not subjected to public disclosure', because of the content and/or nature held within.

Policy

ATSICHS Brisbane collects personal and health information as part of service delivery to service users and includes, but is not limited to:

> *Name, address, phone number, employment and other demographic data, ethnicity, next of kin and family details, social and living circumstances, past medical history, current health issues, and Medicare/Centrelink numbers. This is contained in an electronic medical record which may also contain information received from other sources, e.g., faxes and mail.*

The information is collected for the purpose of providing comprehensive, appropriate and service user-centred health services, additionally personal information will be collected for *other permitted purposes* in line with legal and regulatory requirements.

How we collect information

Staff are to collect information in a fair, lawful and non-intrusive manner. Wherever possible information will be collected directly from the service user (where it is reasonable and practical to do so) rather than from third parties. Information is also collected through:

- forms,
- agreements,
- mail,
- email,
- telephone,
- other health specialists
- our website

At point of service, users are advised of why we are collecting information, any laws that require information to be collected, the types of organisations that we would usually disclose the information to and how to proceed if they have concerns about their privacy being breached.

Wherever lawful and practicable, service users shall be given the option of not identifying themselves or using a pseudonym when engaging with our services. Some services may require the collection of personal information to meet legal, clinical, or funding obligations, in which case anonymity or pseudonymity may not be possible.

Why we collect information

ATSICHS Brisbane collects and uses personal and health information for the primary purpose of providing our services, for example:

- To contact you regarding the delivery of our services
- To make appointments and send reminder notices
- To maintain and update individual service user records
- To provide health information to health professionals in a medical emergency
- To use de-identified information to model or forecast service delivery
- To liaise with a person's nominated representatives or family members where needed
- To improve services through quality improvement activities, audits, surveys and program evaluations
- Information from our website to understand how users interact with our website and to deliver relevant information on social media platforms.

ATSICHS Brisbane may share data with third parties for the purposes of continuous quality improvement, benchmarking and research. ATSICHS Brisbane may disclose information to a third party if the following provisions are met:

- Data is de-identified and aggregated
- A data sharing agreement is in place and approved by the ATSICHS Brisbane Board
- Ethics approvals are in place if relevant
- There is demonstrable benefit for Aboriginal and Torres Strait Islander peoples in South East Queensland in the short, medium or long-term.

Use and disclosure of information

Staff shall only access, use or disclose personal information where the use or disclosure of the information is for the purpose of providing care and treatment to service users and for purposes directly related to providing such care and treatment, e.g., to another health professional.

Disclosure is reasonable and required to complete administrative processes on behalf of service users, such as making appointments, arranging co-payments, or liaising with regulatory authorities (e.g., Medicare). Privacy

laws also permit disclosure in specific circumstances, including compliance with court orders or legislative requirements such as cancer registration, vaccination registers and infectious disease notification. Disclosure may also occur when there is an immediate and specific risk of harm to an identifiable person or persons, and the risk can only be averted by disclosing information.

Students

ATSICHS Brisbane participates in medical, nursing and other student education. It is acknowledged that some service users will not wish their information to be accessed for educational purposes. The clinics advise service users of the presence of students and seek consent accordingly.

Aside from where the law specifically permits, staff will not access, use or disclose information for purposes that are unrelated to the treatment or care of service users, without their consent.

Informing service users about our privacy policy

We inform our service users about our policy regarding the collection and management of their personal information via:

- Signage in receptions and client areas
- Information on our website
- Brochures in receptions and client areas
- New service user forms – 'consent to share information'
- Verbal communication to new service users.

Privacy Complaints

Service users who believe their privacy has been breached may lodge a complaint with ATSICHS Brisbane. All complaints will be acknowledged within two business days and investigated promptly in line with the ATSICHS Brisbane Complaints Policy. Under Queensland's Information Privacy legislation, agencies or their contracted service providers are required to respond to privacy complaints within 45 business days. If unresolved, complaints may be escalated to the Office of the Information Commissioner Queensland (OIC).

Right to Information Complaints

Service users have the right to request access to documents held by ATSICHS Brisbane and by the relevant Queensland Government department under the *Right to Information Act 2009 (Qld)*. This includes:

- Requesting access to most information held by ATSICHS Brisbane or the relevant Queensland Government department.

- Requesting correction of personal information if it is incorrect.
- Requesting a review if you are not satisfied with a decision about your request.

Access to information may be refused if required or permitted by law, including where disclosure would be unlawful, pose a risk to safety, or breach confidentiality provisions.

If a service user believes their request for access has been unfairly refused or mishandled, they may lodge a complaint:

1. Submit a written complaint to ATSICHS Brisbane outlining the concern.
2. ATSICHS Brisbane will respond within 45 business days in accordance with the *Information Privacy Act 2009* and *Right to Information Act 2009*.
3. If unresolved, the complaint may be escalated to the Office of the Information Commissioner Queensland (OIC):
   - Website: www.oic.qld.gov.au
   - Email: administration@oic.qld.gov.au
   - Mail: PO Box 10143, Adelaide Street, Brisbane QLD 4001

If the matter remains unresolved, the complainant may apply to the Queensland Civil and Administrative Tribunal (QCAT) for review.

Requests for Records

ATSICHS Brisbane has a clear process for handling requests for records. All requests must be made in writing and include sufficient information to identify the service user. Proof of identity (or evidence of authority when acting on behalf of another person) is required before any records are released. In some cases, administrative fees may apply to cover the cost of processing and providing copies of records.

Requests for own records

Service users may request access to their information under the APP. ATSICHS Brisbane will provide service users with access to their information unless there is a reason that is listed as an exemption in the relevant APP.

ATSICHS Brisbane strongly prefers that requests are received in writing with an authorising signature from the service user.

Medical record requests are referred to the relevant GP. An appointment will be made, if possible, for the service user and GP to discuss what records are required. ATSICHS Brisbane reserves the right to charge for the administrative work involved in responding to any request to access records. Service users who make a request by phone and are unable to attend an appointment are still eligible to have access to their health records. It is

critical to verify the identity of the service user prior to providing records, regardless of the manner in which the request is received. Each step of the process is to be documented in the service user's chart.

All other service user record requests should be made to the relevant worker and deferred to the operations manager to coordinate the release of them to the service user.

It is important to make service users aware that once a copy of their records has been provided to them (in person, or by post or fax), that ATSICHS Brisbane can no longer be responsible for the privacy of that particular copy of the record.

Requesting review and changes to records

Service users may make requests to correct information in their records if they consider it to be not accurate, up to date and complete. The same process applies as for access to records; it requires an appointment with the relevant GP, or ATSICHS Brisbane worker. For medical, the Senior Medical Officer is to be notified of any requests to change a medical record. For all other services, the relevant operations manager is notified of any requests to change a record.

A request must be responded to with a letter of acknowledgement within 14 days as stated by the National Privacy Commissioner.

If a request for records and/or information is made in relation to correcting and updating current data, records and/or information, the following steps should be reasonably made:

- Gain consent and approval from the individual that the information and record belong to in order to access the required records and/or information before such is changed, added or removed.
- ATSICHS Brisbane will provide notice to the individual which the information or records belong to, specifying:
  - What was changed and altered in anyway
  - What was added
  - What was removed, redacted and/or deleted in anyway
  - When these changes were made
  - Who requested these records and/or information to be changed; either the direct service user and/or someone else.

(i.e., Record/Information _____ *was changed DD/MM/YYYY, HH:MM" by INSERT NAME)*

Requesting records for another person

If a request for records and/or information is made on behalf of another (i.e., a child or individual who is not physically capable to request such records and/or information), steps to verify and establish a connection of the applicant must be adequately made before information is provided. These include:

- The applicant must demonstrate their authority to request such records for that individual
- The applicant may be required to provide identifying documentation of themselves and/or of the person whose records they are requesting, such as a birth certificate, driver's license or Medicare information
- A written statement declaring the applicant is the individual service user, an affidavit, and/or court orders stating guardianship
    - If an applicant is a parent, then ATSICHS Brisbane must reasonably notify the primary guardian parent, at that time, of the attempt to access and request records and or information for that child and/or children.
    - For circumstances involving split parenting, DVOs and court orders, the primary guardian parent must keep ATSICHS Brisbane reasonably updated on reasons as to why the opposing parent should or should not be supplied any or all records and/or information, and if the status of these circumstances are subjected to change at any given point.
    - If permission is given directly from the primary guardian parent, a copy of the record and/or information will be sent to the primary guardian parent, confirming the record and/or information is acceptable and appropriate for the opposing parent to access.
    - If permission is given directly from the primary guardian parent, the primary guardian parent is to confirm with ATSICHS Brisbane on anything within the record and/or information that may need to be redactable information, such as home numbers, mobile phone numbers, residential addresses, billing addresses, billing information, emails and any other form of contact redacted from the record and or information.
    - For circumstances of where records and or information pose a risk to the individual service user, the applicant, or a primary parent and/or guardian, information will either be immediately redacted or otherwise access to such records and or information will be immediately refused.
    - For circumstances involving a deceased service user, ATSICHS Brisbane must appropriately notify the next of kin regarding the access of the service user's records and information, and will confirm whether there are any considerations or reasons the records should not be released.

- The applicant must submit a signed, written request from the owner of the records and/or information, where the request should include, but is not limited to:
  - What specific records and/or information is requested (i.e., blood records)
  - Which workplace department are the records and/or information being requested from? (i.e., Northgate Medical Clinic, Northgate Clinic Nurse)
  - The name of the person, the applicant is requesting records and/or information, (i.e., person/child's full, first, middle and last name)
  - The scope of the request (e.g., whether one record, multiple records, or the entire file is required).
- If a request of medical records is in relation to a legal case or a subpoena/court order, ATSICHS Brisbane may require the applicant for evidence of legal representation linking them to the child.
- A parent and/or legal guardian requesting access to medical records for children over the age of 14, but younger than 18 years, may require consent from the young person to access those records.

If a request of records and/or information is made, organisation and agencies must follow minimum requirements when a request is made. These include:

- Including the time period for responding to a request for access to records and/or information
- Including how access to records and/or information will be given (i.e., hard copy, digital, verbally communicated and/or face-to-face)
- Including access charges and giving written notice to when records and/or information are made. In the event that someone else who has not been given authority, permission or adequate consent from the direct service user attempts to access records and/or information.
- Including if applicable, refusal to give access to records and/or information within reasonable limitations (i.e., see 'Authority to refuse access').

Authority to refuse access

ATSICHS Brisbane may have the authority to refuse access to anyone who requests records and information if these meet specific circumstances, which include but are not limited to:

- if giving access would be unlawful in any way, shape, or form
- if the document is an exempt document that is subject to legal professional privilege, contains matter obtained in confidence, or a secrecy provision applies

- if denying access is required or authorised by or under an Australian law or a court/tribunal order
- if ATSICHS Brisbane reasonably believes giving access would pose a serious threat to the life, or health and safety of any individual service user, or to public health or public safety
- if the request is frivolous or vexatious
- if giving access would likely prejudice the taking of appropriate action in relation to suspected unlawful activity or serious misconduct
- if giving access would likely prejudice a performance related activity conducted by or on behalf of an enforcement body.

If ATSICHS Brisbane is concerned that the release of records and/or information may risk causing harm to the individual service user, including children, we may have the right to decline the request for records.

ATSICHS Brisbane may need to seek legal advice about the provision and access of medical records if uncertain.

Requests for transfer of medical records to other medical services or to legal entities

Records are sent only upon receiving a request from the other practice signed by the service user. If necessary, an invoice is issued by ATSICHS Brisbane to the requesting party. The GP approves the transfer of records, and they are sent using secure methods. This may include transfer via encrypted secure storage systems, SharePoint (with controlled access), fax, or registered mail. Where possible, secure electronic transfer is the preferred method.

Records may also be released without consent where required by law, such as in response to a valid subpoena, court or tribunal order, or statutory obligation. These are lawful requests, and they are managed in the same way – invoice, GP approval and secure mode of transfer.

International – information may be sent overseas with service user consent, but the clinic is under no obligation to supply any service user information upon receipt of an international subpoena.

Privacy infringements

All ATSICHS Brisbane employees and visiting health professionals are bound by the privacy clause contained within the Employment Agreement (staff) and the Contractor, Student and Temporary employee induction document (others), which is signed at commencement of employment. Under no circumstances are employees to discuss or in any way reveal service user information or documentation to unauthorised staff, colleagues, other service users, family or friends, the community or the broader public, whether within the clinic or outside it, i.e., at home or socially. Infringements that are substantiated will result in disciplinary action in accordance with ATSICHS Brisbane's Managing Poor Performance and Disciplinary Policy.

Data security and retention

Personal information is kept in electronic form and is controlled, monitored and restricted to relevant staff and authorised external users only. Security safeguards are in place to ensure information is protected against loss, interference or modification, and unauthorised access or misuse. ATSICHS Brisbane keeps service user records in accordance with the Australian Privacy Principles (APP11) and destroys/de-identifies records as appropriate for the service that holds them. ATSICHS Brisbane retains personal and health information for the minimum periods required by Queensland law and Commonwealth legislation, generally at least seven years from last contact or until a child turns 25, whichever is longer.

Where a service user requests deletion, we will assess any legal or contractual retention obligations. If none apply, information will be securely destroyed or de-identified. If retention is required, it will be restricted from active use and destroyed or de-identified at the earliest lawful opportunity.

Before ATSICHS Brisbane discloses your data, records and/or service user information to another business, we will notify you as reasonably applicable, specifying:

- What information was disclosed
- How much information was disclosed
- When this information was disclosed
- Which business the information was disclosed to.

If ATSICHS Brisbane receives data, records and/or information about you that is solicited, we will notify you as reasonably applicable, specifying:

- What information was received
- How much information was received
- When this information was received
- Which business the information was received from.

Data breach

Any breach of data will be assessed as per the *Privacy Amendment (Notifiable Data Breaches) Act 2016* using the ATSICHS Brisbane Data Breach Response Plan. This is to ensure breaches are appropriately dealt with and notified to the individual(s) concerned and the Office Australian Information Commissioner (OAIC) where necessary. Where an eligible breach is confirmed, ATSICHS Brisbane will take all reasonable steps to notify affected individuals as soon as practicable, and no later than 30 days after the breach is identified.

If ATSICHS Brisbane receives data, records and/or information about you that is unsolicited and was disclosed without your consent, we will ensure that the data will be destroyed immediately, as reasonably practicable, unless a law or court order requires the data, records and/or information to be retained.

If a data breach occurs, ATSICHS Brisbane will provide reasonable notification to affected service users. This notification will include:

- What records or information were breached
- What specific information was involved
- What the situation was
- Recommendations ATSICHS Brisbane will undertake in response to the breach.

ATSICHS Brisbane NDIS users and Privacy

ATSICHS Brisbane is subject to NDIS (Quality and Safeguards) Commission Rules and Regulations. ATSICHS Brisbane will follow the guidelines of the Australian Privacy Principles in its information management practices.

ATSICHS Brisbane will advise each participant of privacy policies using the language, mode of communication and terms that the participant is most likely to understand (Easy Read documents are made available to all participants).

Work procedures to ensure privacy

All ATSICHS Brisbane staff have a responsibility to uphold the privacy and confidentiality of service user health information, and this is reflected in everyday procedures and processes:

- Care is to be taken so that the general public cannot see or access computer screens that display information about other individuals. To minimise this risk, automated screen savers are engaged, as are screen covers that allow no sideways visual access.
- Documents containing personal information are to be kept out of view in areas where staff are always present. They are not to be left in public or unattended areas.
- Staff members are provided different levels of access to user information as appropriate. To protect the security of health information, clinic staff do not give their computer passwords to anyone.
- Conversations between staff about users are to be conducted away from public areas using discretion.
- Conversations with service users at the front desk or phone calls to service users from the front desk are to be conducted in quiet voices and with minimal personal or identifying information.

- Email is generally not considered to be secure as there is the possibility of it being intercepted. Sensitive user information is only to be sent via email if it is securely encrypted according to industry standards, e.g., Medical Objects, MMex internal messaging.
- Service user privacy and security of information is maximised during consultations by closing consulting room doors. Clinic staff wishing to enter a room in which a consultation is underway must knock and wait or phone through to the relevant person in the room.
- During consultations, care is taken not to disclose personal information when another service user is present in the room when a phone call is received. Unless it is an urgent medical issue, a clinician should not take a phone call relating to a service user whilst consulting with a different service user.
- Handling of paper documents and correspondence:
  - For medical clinics, incoming service user correspondence and diagnostic results are opened by reception staff and placed in designated trays out of view ready for review or scanning.
  - Where service user information is sent by post, the use of registered post or a courier service is determined on a case-by-case basis.
  - Items for collection or postage are left in a secure area not in the view of the public.
  - Any documents containing service user information are shredded after scanning into the service user's electronic record.
  - Items are faxed with the transmission report sheet providing confirmation of the successful transmission to the correct fax number.
  - All staff must identify our service users using three service user identifiers – name, date of birth, address or phone number to ascertain we have the correct service user record before entering or actioning anything from that record.
  - NDIS participant records are kept confidential and only handled by staff directly engaged in the delivery of service to the participant. Information about participants may only be made available to other parties with the consent of the participant, or their advocate, guardian or legal representative. All participant records will be kept on a securely protected database that is restricted to staff members directly engaged in the delivery of service to the participant.
  - All hard copy files of service user records will be kept securely in a locked filing cabinet.

Legislative References

- *The Privacy Act 1988 (Cth) ('Privacy Act')*

- Australian Privacy Principles ('APPs') as per *Privacy Amendment Act*, forming part of the *Privacy Act 1988*
- RACGP 6th edition standards 1.1 and 6.3
- *Privacy Amendment (Notifiable Data Breaches) Act 2017*
- *National Disability Insurance Scheme Act 2013*
- Queensland Government Human Services Quality Standards
- *Information Privacy Act 2009 (Qld)*
- Queensland Privacy Principles (QPPs)
- *Right to Information Act 2009 (Qld)*

Related Resources and Documentation

- Code of Conduct Policy (doc_187)
- Grievance Resolution Policy (doc_154)
- ICT Security Policy (doc_142)
- Client Information Pack - Community Services (doc_0764)
- ATSICHS Data Breach Response Plan (doc_1671)
- Transfer of Clinical Records to Non-Medical Entities Policy & Procedure (doc_1077)
- NDIS Practice Standards and Quality Indicators 2018
- RACGP computer and information security standards. http://www.racgp.org.au/your-practice/standards/computer-and-information-security-standards/
- Dignity and Respect / Privacy and Confidentiality policy (LASA)