PRIVACY AND DIGNITY POLICY AND PROCEDURE

PURPOSE

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 collects and manages personal information. It also seeks to ensure that ATSICHS 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.

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
- RACGP5th 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

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)

POLICY

ATSICHS Brisbane collects personal and health information as part of our 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, mail.*

The information is collected for the purpose of providing comprehensive, appropriate and service user-centered health services, additionally personal information will be collected for *permitted purposes* in line with COVID 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, and other health specialists. 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 to whom we would usually disclose the information and how to proceed if they have concerns about their privacy being breached.

WHY WE COLLECT INFORMATION

ATSICHS collects and uses personal and health information for the primary purpose of providing our services e.g.

- 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.

ATSICHS may share data with third parties for the purposes of continuous quality improvement, benchmarking, and research. ATSICHS 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 Board of Directors
- Ethics approvals are in place if relevant
- There is demonstrable benefit for Aboriginal and Torres Strait Islander people 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, e.g. to make appointments, arrange co-payments, liaise with regulatory authorities (e.g. Medicare). Privacy laws permit disclosure for specific circumstances, e.g. court orders and legislative requirements such as cancer registration, vaccination registers and infectious disease notification. Disclosure will also occur when there is an immediate and specific risk of harm to an identifiable person or persons that can be averted only by disclosing information.

STUDENTS

ATSICHS 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 which are unrelated to the treatment of care of service users, without the consent of a patient.

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:

- A sign at receptions and client areas
- Information on the Website
- Brochures in receptions and client areas
- New Service User forms – 'consent to share information'
- Verbally to new service users.

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 by fax or by registered mail.

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.

SUBPOENA OR COURT ORDER FOR RECORDS

These are lawful requests and they are managed in the same way – invoice, GP approval and secure mode of transfer.

PRIVACY INFRINGEMENTS

All ATSICHS 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 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, unauthorised access or misuse. ATSICHS keeps service user records in accordance with the Australian Privacy Principles (APP11) and destroys/de-identifies records as appropriate for the service which holds them.

Data Breach

Any breach of data will be assessed as per the Privacy Amendment (Notifiable Data Breaches) Act 2016 using the ATSICHS 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.

Service user access to records

Service users may request access to their information under the APPs. ATSICHS 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 strongly prefers that requests are received in writing with an authorising signature from the service user.

For medical records requests they 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 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 who are unable to attend for 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 users 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, by post or fax) that ATSICHS can no longer be responsible for the privacy of that particular copy of the record.

SERVICE USERS WANTING TO MAKE 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 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.

ATSICHS NDIS USERS AND PRIVACY

Aboriginal and Torres Strait Islander Community Health Service Brisbane is subject to NDIS (Quality and Safeguards) Commission Rules and Regulations. Aboriginal and Torres Strait Islander Community Health Service Brisbane will follow the guidelines of the Australian Privacy Principles in its information management practices.

Aboriginal and Torres Strait Islander Community Health Service 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).

RELATED FORMS, POLICIES, PROCEDURES & DOCUMENTATION

- Code of conduct policy (doc_187)
- Grievance resolution procedure policy (doc_154)
- Brisbane ITC security policy (doc_142)
- 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/
- Service user information sheet – Your Privacy.
- Transfer of Clinical Records to Non-Medical Entities Policy
- Client Information Pack Human Services
- ATSICHS Data Breach Response Plan

- Privacy and Confidentiality Agreement
- Dignity and Respect / Privacy and Confidentiality policy (LASA)

WORK PROCEDURES TO ENSURE PRIVACY

All ATSICHS 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 that the general public cannot see or access computer screens that display information about other individuals. To minimize 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 a front desk, or phone calls to service users from a 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.
- Consultations - Service user privacy and security of information is maximized 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.
- Phone calls 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 view of the public.
    - Any document 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 3 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.
    - Participant records will be 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 cabinets.