

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 2012. 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

Definitions

'Consent' is defined as '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

Legislative References

- Federal Privacy Act 1988
- Australian Privacy Principles (APPs) as per Privacy Amendment Act 2012, forming part of the Privacy Act 1988
- RACGP 4th edition standards 4.2.1 and 3.1.4
- APP 12 Access to information 2014.

Policy

ATSICHS Brisbane collects the following personal and health information as part of our service delivery to clients:

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 solely for the purpose of providing comprehensive, appropriate and client-centered health services. [How we collect information](#)

Staff will endeavor to collect information in a fair, lawful and non-intrusive manner. Wherever possible information will be collected directly from the patient (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. Information will be provided to patients advising them 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 the consequences of not providing information.

Why we collect information

ATSICHS collects and uses personal and health information for the primary purpose of providing health services and managing health conditions, for example, to:

- make appointments and send reminder notices
- maintain and update individual client records
- provide health information to health professionals in a medical emergency
- use de-identified information to model or forecast service delivery
- liaise with a person's nominated representatives or family members where needed
- improve services through quality improvement activities, audits, surveys and program evaluations.

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 patients 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 patients, 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.

Students

ATSICHS participates in medical, nursing and other student education. It is acknowledged that some clients will not wish their information to be accessed for educational purposes. The clinics advise clients 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 patients, without the consent of a patient.

Informing clients about our privacy policy

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

- A sign at reception
- Information on the Website
- Brochures in reception
- New client forms – 'consent to share information'
- Verbally to new clients.

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

ATSICHS has a procedure for managing these. Records are sent only upon receiving a request from the other practice, signed by the client. 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 client consent, but the clinic is under no obligation to supply any client 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 client information or documentation to unauthorized staff, colleagues, other clients, 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 may provide grounds for disciplinary action or dismissal.

Data Security and Retention

Personal information is kept in electronic form and is controlled, monitored and restricted to relevant staff and authorized external users only. Security safeguards are in place to ensure information is protected against loss, interference or modification, unauthorized access or misuse. ATSICHS Brisbane keeps records indefinitely, as electronic records are made inactive rather than destroyed as such.

Client access to records

Clients may request access to their health information under the Australian Privacy Principles (APPs). ATSICHS Brisbane will provide clients 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 authorizing signature from the client. All requests are referred to the relevant GP. An appointment will be made (if possible) for the client 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.

Requests received by a phone call from a client who is 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 client 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 clients chart.

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

Clients wanting to make changes to records

Clients may make requests to correct information in their health record 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. The Senior Medical Officer is to be notified of any requests to change a medical record.

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

Related forms, policies, procedures & documentation

- *Privacy Act 1998*
- Code of conduct policy (doc_187)
- Grievance resolution procedure policy (doc_154)
- Brisbane ITC security policy (doc_142)
- RACGP computer and information security standards: www.racgp.org.au/your-practice/standards/computer-and-information-security-standards/
- Transfer of medical records procedure (not yet complete)

Work procedures to ensure privacy

All ATSIHCS Brisbane staff have a responsibility to uphold the privacy and confidentiality of client 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 health 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.
- Members of the clinic team are provided different levels of access to client health information. To protect the security of health information, clinic staff do not give their computer passwords to anyone.
- Conversations between clinic staff about clients are to be conducted away from public areas using quiet voices.
- Conversations with clients at the front desk, or phone calls to clients 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. Client 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 - Client 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 client 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 client whilst consulting with a different client.

Handling of paper documents and correspondence

- Incoming client correspondence and diagnostic results are opened by reception staff and placed in designated trays out of view ready for review or scanning.
- Where medical 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.
- Documents that contain client information are shredded after scanning into the client's electronic record.
- Items are faxed by reception staff with the transmission report sheet providing confirmation of the successful transmission to the correct fax number.
- All clinic staff must identify our clients using 3 client identifiers – name, date of birth, address or phone number to ascertain we have the correct client record before entering or actioning anything from that record.