Privacy & Confidentiality Policy

Purpose

The purpose of this policy is to ensure that all personal, sensitive and health-related information collected by IWC is managed lawfully, ethically, and securely. This includes information collected, stored, or processed through traditional records and patient management systems, digital platforms, and emerging technologies such as artificial intelligence (AI).

The policy ensures compliance with the Privacy Act 1988, the Australian Privacy Principles (APPs) and all other legislative, regulatory, and accreditation requirements relevant to IWC.

Scope

This policy applies to:

- All personal information collected, stored, used, and disclosed by IWC.
- All employees, contractors, students and volunteers.
- All programs and services provided under health, dental, allied health, NDIS, aged care, child safe and community services.
- All technologies and systems, including electronic records, AI applications, and communication platforms.

References

ISO 9001:2015 Quality Management Systems

RACGP Standards for General Practices 5th Edition (Medical)

National Safety and Quality Primary and Community Healthcare Standards (Dental)

Commonwealth Home Support Programme (Home Care)

Privacy Act 1988 and other Legislation Amendment Acts (Cth)

Australian Privacy Principles (APP)

Community Services Act 2007

Public Health Act 2005

Aged Care Act 1997 (Cth)

Child Protection Act 1999 (Qld) and National Principles for Child Safe Organisations

QA-POL-022 AI Guiding Policy

Responsibility

All IWC employees are responsible for maintaining confidentiality and complying with this policy.

Quality Assurance Manager ensures compliance with the Privacy Act, APPs, and all accreditation requirements. QA Manager also oversees implementation, incident management, and data breach notifications.

Information Services (IS) ensures secure data storage, system access, and monitoring of AI technologies.

Definitions

Clients – includes patients, customers, clients and participants.

Employees – includes staff, contractors, and students.

IWC – Indigenous Wellbeing Centre is our Organisation.

Policy

Collection of Information

IWC collects personal and sensitive information only when essential to deliver health, disability, aged care, dental, allied health, and community services. Collection is conducted lawfully, fairly, and in line with professional standards.

With written or documented verbal consent, information may also be collected from other providers or agencies to ensure continuity of care.

Use and Disclosure of Information

Personal information will not be disclosed except where:

- Informed consent is provided by the individual or their authorised representative.
- Required by law (e.g. Public Health Act 2009 notifiable conditions).
- Necessary to protect a child, vulnerable adult, or other person from harm, consistent with child safe, aged care, and NDIS safeguarding responsibilities.
- An emergency exists where duty of care requires disclosure.

IWC does not sell, rent, or trade client information. Information is used only for the purposes for which it was collected, unless authorised by law.

Confidentiality and Records Management

All personal and health information, whether in hard copy or digital form, will be securely stored and protected against loss, misuse, or unauthorised access. Volunteers do not have individual logins to access client records, although they may be privy to information. Staff are trained and accountable for upholding confidentiality obligations. All staff and volunteers sign a Confidentiality Agreement prior to commencing.

Clients are informed at the time of entry into services about the types of information collected, why it is collected, and their rights to access and correct their records.

Record Retention Principles

- Legal Compliance: Retain records in accordance with the Public Records Act 2023 (Qld), approved retention & disposal schedules, Privacy Act 1988 (Cth), and sector-specific requirements (e.g., NDIS, clinical records).
- Purpose Limitation: Keep records only as long as necessary for business, legal, clinical, or regulatory purposes.
- Retention Timeframes:
    - Adult client records: minimum 10 years after last service
    - Minor client records: until 10 years after turning 18
    - Administrative, financial, and corporate records: generally minimum 7 years or as required by law/schedule

- Secure Storage & Disposal: Store records securely; destroy or de-identify them when no longer required, in line with schedules and privacy obligations.

Role-Based Access to Information

IWC applies role-based access controls (RBAC) to ensure that access to personal, health, and sensitive information is:

- Appropriate to a person's role
- Limited to what is necessary
- Used for a legitimate work-related purpose

Access to information is granted in accordance with the principle of:

- Right person, right access, right reason

This means that staff, volunteers, and authorised third parties may only access information where:

- The access is directly related to their role or delegated responsibilities
- The access is necessary to perform their duties
- There is a legitimate business, clinical, or service delivery purpose

Artificial Intelligence (AI) Use

Where AI technologies are used to support service delivery (e.g. transcription, communication, or documentation tools):

- Clients will be informed, and consent will be obtained before their information is processed using AI.
- AI-generated records will be reviewed, verified, and authorised by a qualified staff member before becoming part of the client record.
- AI will not be used for profiling, automated decision making, or voice cloning without explicit written consent.
- AI systems will comply with Australian privacy and security standards, and all data will be deleted after secure transfer to official records.

Only AI tools approved by IWC and governed by Information Services are to be used for processing any client or personal information. Please refer to QA-POL-022 AI Guiding Policy for more information.

Data Breaches

IWC will:

1. Contain and assess any suspected or actual data breach.
2. Evaluate the risk using the organisational risk matrix.
3. Notify affected individuals where the breach is likely to result in serious harm.
4. Report notifiable breaches to the Office of the Australian Information Commissioner (OAIC) as required under the Privacy Amendment (Notifiable Data Breaches) Act 2017.
5. Implement corrective actions to prevent recurrence.

Training and Compliance

All employees receive training on privacy, confidentiality, child safety, aged care safeguarding, disability rights, and information management. Annual refresher training is mandatory.

Breaches of this policy may result in corrective or disciplinary action, and in serious cases, may be referred to regulatory authorities.

Client Rights

Clients have the right to:

- Access their personal information within legislation and after IWC assessment of the request.
- Request corrections to ensure accuracy.
- Withdraw consent for certain uses of their information (unless required by law).
- Complain about privacy concerns, with the assurance that complaints will be investigated and responded to in a timely and transparent manner.

Please note that **all** requests for Personal Health information must go to Privacy team first.