

Introduction

SWAMS is committed to protecting the privacy of client / patient information and to handling personal information in a responsible manner in accordance with the Privacy Act 1988 (Cth), the Privacy Amendment (Enhancing Privacy Protection) Act 2012, and the Australian Privacy Principles.

This policy explains how:

- personal information is collected, used and disclosed,
- a person may access that information
- how to seek the correction of any information.

It also explains how to make a complaint about a breach of privacy legislation.

PART A: Policy Information

Evidence Base

- RACGP C6.3 and C6.4
- Privacy Act 1988
- Privacy Amendment (Enhancing Privacy Protection) Act 2012
- NDIS (Quality Indicators) Guidelines 2018
- Aged Care Quality and Safety Framework and Standards
- Australian Privacy Principles (APPs)
 - Consideration of personal information (APPs 1 and 2)
 - Collection of personal information (APPs 3, 4 and 5)
 - Dealing with personal information (APPs 6, 7, 8 and 9)
 - Integrity of personal information (APPs 10 and 11)
 - Access to and correction of personal information (APPs 12 and 13)

Linked Documents

- SWA-HR-T02- Confidentiality Agreement
- SWA-HR-P06 - SWAMS Employee Handbook – (Section 18)
- SWA-CS-F12- Contractor Declaration of Confidentiality
- SWA-HR-F27- Student Declaration of Confidentiality
- SWA-CL-P29- Third Party Requests for Access to Medical Records
- SWA-CS-P28- Data Breach Policy
- SWA-HR-P20- Code of Conduct
- SWA-CL-P18- Open Disclosure
- SWA-CS-P29- Corrective and Preventative Actions
- SWA-CS-F19- Consent for Use of Images Videos and Recordings
- Cultural Sensitivity In The Use of Images Videos and Recordings Policy and Guidelines
- SWA-CS-P12- Service Provider Compliance
- SWA-HP-F08#2- NDIS Agreement

Purpose

- This policy is to provide information on how a clients personal information (including health information) is collected and used by SWAMS and the circumstances under which it may be shared with third parties.

Scope – Personally Identifiable Data

The following programs define the scope of data that falls under this policy:

- Communicare
- Clinic Case Management Files – E.g. Flinders Information
- ETrack
- Human Resource Staff Files
- ASICAbcorp
- SWAMS Membership List
- Employment HERO
- Visual Care
- Netsuite
- SWAMS S:Drive, T:Drive, Sharepoint

Definitions

Client

- For the purposes of this policy the term 'client' is used to describe the person receiving SWAMS services. (in lieu of 'patient', 'consumer', 'participant' or 'service recipient'.)

Responsibilities

Senior Leadership Team (CEO and Directors)

- Support the implementation of the Privacy and Confidentiality Policy

Managers

- Identify and implement privacy and confidentiality processes in their area of responsibility
- Ensure employees are aware of the privacy and confidentiality protocols in their area of responsibility

Employees and Contractors

- Ensure they practice the privacy and confidentiality protocols within their working environment
- Cooperate with data breach investigations as required.

Part B: Personal Information

When a person registers as a client (or patient) they grant consent for SWAMS to access and use personal information. Only those who require access to personal information will receive it.

The main purpose for collecting, using, holding and sharing personal information is to manage a client's physical health, social, emotional wellbeing, mental health, Disability and Aged Care service delivery. It is also used for directly related business activities, such as financial claims and payments, practice audits and accreditation, and business processes (e.g. staff training).

Information includes:

- Name, date of birth, addresses, contact details
- Medical information including medical history, medications, allergies, adverse events, immunisations, social history, family history and risk factors
- Personal information related to disabilities and the National Disability Insurance Scheme (NDIS).
- Personal information related to Aged Care services, including MyAged Care, RAS assessments and ACAT assessments
- Medicare number (where available) for identification and claiming purposes

- Healthcare identifiers
- Health fund details

In accordance with the Privacy Act, a client has the right to remain anonymous or under to register under a pseudonym unless it is impracticable, or unless there is a requirement by law to only engage with identified individuals. (APP2)

SWAMS may collect personal information in several different ways:

- a) When a client makes an initial appointment personal information and demographic information will be collected via the registration. (Ref: Policy New Client Registration SWA-CL-P03)
- b) During the course of delivering services, SWAMS may collect further personal information. This could include, but is not limited to such eHealth services such as electronic transfer of prescriptions (eTP), My Health Record, e.g. via Shared Health Summary, Event Summary, NDIS information or Aged Care information via MyAgedCare.
- c) SWAMS may also collect personal information from visitors to the website or other social media is used, including emails, SMS, telephone calls or online appointments
- d) In some circumstances personal information may also be collected from other sources. Often this is because it is not practical or reasonable to collect it from the client directly. This may include information from:
 - A guardian, Enduring Power of Attorney or Enduring Power of Guardianship
 - Other involved healthcare providers, such as specialists, allied health professionals, hospitals, community health services and pathology and diagnostic imaging services, or pharmacies.
 - The patients' health fund, Medicare, or the Department of Veterans' Affairs (as necessary).

SWAMS may be required to share personal information under the following conditions:

- With third parties who work with SWAMS for business purposes, such as accreditation agencies or information technology providers – these third parties are required to comply with APPs and this policy
- With other healthcare providers
- When it is required or authorised by law (E.g. court subpoenas)
- When it is necessary to lessen or prevent a serious threat to a client's life, health or safety or public health or safety, or it is impractical to obtain the client's consent
- To assist in locating a missing person
- To establish, exercise or defend an equitable claim
- For the purpose of confidential dispute resolution process
- When there is a statutory requirement to share certain personal information (E.g. some diseases require mandatory notification)
- During the course of providing medical services, through eTP, My Health Record (E.g. via Shared Health Summary, Event Summary)
- With third parties with whom SWAMS has a research or other partnership with as part of a formal agreement and information will not be shared without the formal consent of the client.

Only those who need to access client information will be able to do so. Other than in the course of providing medical services or as otherwise described in this policy, SWAMS will not share personal information with any third party without consent of a Client. (*Refer: Third Party Requests for Access to Medical Records – SWA-CL-P29*)

SWAMS will not share personal information with anyone outside Australia (unless under exceptional circumstances that are permitted by law) without client consent.

SWAMS will not use personal information for marketing goods or services directly to a client without express consent from the patient. If a client does consent, they may opt out of direct marketing at any time by notifying SWAMS in writing.

Part C: Storage and Access to Personal Information

Personal information is stored and protected in various forms:

- Health records, where applicable, are stored electronically. Otherwise they are kept in secure locations with limited access
- Computer screens are positioned so that personal information cannot be seen
- Access to computerised client personal information is strictly controlled with passwords, personal logins and other data controls
- Automatic screen savers and computer terminals are logged off when the computer is left unattended for a significant period of time
- Items for pathology couriers or other pickups are left behind the reception desk
- Appropriate Director allocates IT access level at the delegation of the CEO
- All employees are required to sign a Confidentiality Agreement on commencement of employment and further information is provided in Human Resource management
- If transporting confidential information between sites, vehicles or when working from home, all information should be stored in a locked briefcase/bag for transport purposes and confidentially stored overnight in locked cabinets or briefcases/bags at all times. Confidential information should not be left unattended in a vehicle between the workplace and home.

Clients have the right to request access to, and correction of, their personal information which is done in writing. SWAMS will respond within a reasonable time, but no longer than 30 working days from the date of receiving the request and will take reasonable steps to correct personal information where the information is not accurate or up to date.

From time to time, SWAMS may seek clarification of client details to ensure accuracy to client personal information.

Part D: Complaints

SWAMS takes feedback, complaints and concerns regarding privacy and confidentiality very seriously. All privacy and confidentiality concerns are made formally in writing or is a culturally appropriate way that provides “gravitas” to the issue. SWAMS will undertake an investigation of process to resolve the issue in line with policy “SWA-CS-P11Client Feedback and Complaints”

A client may also be directed to contact the OAIC, NDIS, NDIS Quality and Safeguarding Commission or Aged care Quality and Safety Commission.

Part E: Privacy and SWAMS Website

SWAMS utilises social media sites from time to time, to interact and communicate with clients, potential clients and the general community and although SWAMS currently does not directly collect information from these sites, any interaction within this medium is collected via cookies by the communication medium, and at any time may be accessed by SWAMS.

Part F: Compliance

This policy ensures SWAMS protects and manages personal information in accordance with the **NDIS** and **Aged Care** requirements and relevant privacy legislations. An individual’s right to privacy is recognized and respected, while recognising that personal information is required to be collected, maintained and administered in order to provide a safe working environment and a high standard of quality.

The information collected is used to provide services to clients in a safe and healthy environment with

individual requirements to:

- meet duty of care obligations
- initiate appropriate referrals
- conduct business activities to support those services.

To support the privacy and confidentiality of clients SWAMS is:

- committed to complying with the privacy requirements of the Privacy Act, the Australian Privacy Principles and for Privacy Amendment (Notifiable Data Breaches) as required by organisations providing disability services, and aged care services
- fully committed to complying with the consent requirements of the NDIS Quality and Safeguarding Framework and relevant state or territory requirements

We provide all clients with access to information about the privacy of their personal information and they have the right to opt out of consenting to, and providing their personal details if they wish. They also have the right to access their personal records.

Where SWAMS is required to report to government funding bodies, information provided is de-identified and is related to services, support hours provided, age, disability, language, and nationality. Clients may be approached to contribute to external audits if they wish.

Personal information is only used by SWAMS and will not be shared externally without permission unless required by law (e.g. reporting assault, abuse, neglect, or where a court order is issued) images or video footage of participants will not be used without consent.

Part G: Security of information and Data Breaches

To keep information secure, SWAMS takes reasonable steps to protect the personal information held against misuse, interference, loss, unauthorised access, modification and disclosure.

Security of personal information includes password protection for IT systems, locked filing cabinets and physical access restrictions with only authorised personnel permitted access. Personal information no longer required is securely destroyed or de-identified.

As part of information security responsibilities SWAMS takes reasonable steps to reduce the likelihood of a data breach occurring including storing personal information securely and accessible only by relevant employees. If a breach is suspected where personal information has been accessed by unauthorised parties, and could cause harm, reasonable steps will be taken to reduce the chance of harm and advise clients of the breach, and if necessary, the Office of the Australian Information Commissioner.