Introduction

SWAMS is committed to protecting the privacy of 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 we collect, use and disclose personal information, how a person may access that information and how a person may 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 (Cth)
- 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

- Confidentiality Agreement – Doc 788
- SWAMS Employee Handbook – Doc 545 (Section 18)
- Contractor Declaration of Confidentiality – Doc 634
- Student Declaration of Confidentiality – Doc 786
- Data Breach Policy – Doc 636

Purpose

- This policy is to provide information on how personal information (which includes health information) is collected and used within our practice, and the circumstances in which we may share it 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

- Human Resource Staff Files
- Office of the Registrar of Indigenous Corporations
- Abcorp
- SWAMS Membership List
- MyRecruitmentPlus recruitment system
- WageEasy
- Time Target
- MYOB
- SWAMS S:Drive

Definitions

- No definitions have been applied to this policy

Responsibilities

Directors and CEO

- Support the implementation of the Privacy and Confidentiality Policy

Management

- 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

Why and when consent is necessary

When a person registers as a patient they provide consent for our GPs and practice staff to access and use personal information. Only staff who need to see personal information will have access to it. If we need to use information for anything else, we will seek additional consent from the patient to do this.

Why do we collect, use, hold and share personal information

Our main purpose for collecting, using, holding and sharing personal information is to manage a patient's health. We also use it for directly related business activities, such as financial claims and payments, practice audits and accreditation, and business processes (E.g. staff training).

What personal information do we collect?

The information we will collect about patients includes:

- Names, date of birth, addresses, contact details

- Medical information including medical history, medications, allergies, adverse events, immunisations, social history, family history and risk factors
- Medicare number (where available) for identification and claiming purposes
- Healthcare identifiers
- Health fund details
- Personal information related to disabilities and the National Disability Insurance Scheme (NDIS.

Dealing with us anonymously

In accordance with the Privacy Act, a patient has the right to deal with us anonymously or under a pseudonym unless it is impracticable for us to do so, or unless we are required or authorized by law to only deal with identified individuals. (APP2)

How do we collect personal information?

Our practice may collect personal information in several different ways.

a) When a patient makes an initial appointment our practice staff will collect personal and demographic information via the registration. (Ref: Policy New Client Registration doc_084)

b) During the course of providing medical services, we 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.

c) We may also collect personal information when a patient visits our website, sends us an email or SMS, telephones us, makes an online appointment or communicates with us using social media.

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 patient directly. This may include information from:

- A guardian or responsible person
- Other involved healthcare providers, such as specialists, allied health professionals, hospitals, community health services and pathology and diagnostic imaging services, or pharmacy's
- The patients' health fund, Medicare, or the Department of Veterans' Affairs (as necessary).

When, why and with whom do we share personal information?

We sometimes share personal information under the following conditions:

- With third parties who work with our practice 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 patient's life, health or safety or public health or safety, or it is impractical to obtain the patient'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 we have 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 people who need to access patient information will be able to do so. Other than in the course of providing medical services or as otherwise described in this policy, our practice will not share personal information with any third party without consent of a patient. *(Refer: Third Party Requests for Access to Medical Records – doc_77)*

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

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

Part C: Storage and access to personal information

How do we store and protect personal information?

Patient personal information may be stored and protected at our practice in various forms.

- Health records must be kept where constant staff supervision is easily provided. Personal health information must be kept out of view and must not be accessible by the public.
- Health records where applicable are stored electronically
- Computer screens are positioned so that individuals cannot see information about other individuals
- Access to computerised client information is strictly controlled with passwords and personal logins
- 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
- Clinical Director allocates IT access level at the delegation of the CEO
- Each staff member must 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.

How can patients access and correct personal information at our practice?

Patients have the right to request access to, and correction of, their personal information.

Our practice acknowledges patients may request access to their medical records. We require this request be in writing, and our practice will respond within a reasonable time, but no longer than 30 working days from the date of receiving the request.

Our practice will take reasonable steps to correct personal information where the information is not accurate or up to date. From time to time, we will ask a patient to verify that personal information held by our practice is correct and current. A patient may also request that we correct or update their information, and as such requests should also be made in writing.

Part C: Complaints

How can a patient lodge a privacy related complaint and how will the complaint be handled?

We take complaints and concerns regarding privacy seriously. A patient should express any privacy concerns they may have in writing. We will then attempt to resolve it in accordance with our resolution procedure. (Ref: Client Feedback and Complaints doc_603)

A patient may also be directed to contact the OAIC. For further information visit www.oaic.gov.au or call the OAIC on 1300 363 992.

Part D: Privacy and our website

SWAMS utilises social media sites from time to time, to interact and communicate with patients. 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 E: NDIS Compliance

This policy ensures we protect and handle personal information in accordance with the NDIS and relevant privacy legislation. We acknowledge an individual's right to privacy 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 we collect is used to provide services to participants in a safe and healthy environment with individual requirements, to meet duty of care obligations, to initiate appropriate referrals, and to conduct business activities to support those services.

SWAMS commitment to NDIS participants

To support the privacy and confidentiality of individuals:

- We are 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
- We are fully committed to complying with the consent requirements of the NDIS Quality and Safeguarding Framework and relevant state or territory requirements
- We provide all individuals with access to information about the privacy of their personal information
- Each individual has the right to opt out of consenting to and providing their personal details if they wish
- Individuals have the right to request access to their personal records by requesting this with their contact person
- Where we are required to report to government funding bodies, information provided is non-identifiable and related to services and support hours provided, age, disability, language, and nationality
- Personal information will only be used by us and will not be shared outside the organisation without your 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 their consent participants have the option of being involved in external NDIS audits if they wish.

Security of information

To keep information secure:

- We take reasonable steps to protect the personal information we hold against misuse, interference, loss, unauthorised access, modification and disclosure
- Personal information is accessible to the participant and is able for use only by relevant workers
- Security for 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.

Data breaches

As part of information security responsibilities:

- We will take reasonable steps to reduce the likelihood of a data breach occurring including storing personal information securely and accessible only by relevant workers
- If we know or suspect your personal information has been accessed by unauthorised parties, and we think this could cause you harm, we will take reasonable steps to reduce the chance of harm and advise you of the breach, and if necessary, the Office of the Australian Information Commissioner.