

Occupational Therapy – in and out of hospital

Inge Steinhoff, MSc OT (UCT)

Tel. 076 339 8063

Email: inge.steinhoff@gmail.com

www.neurorehabathome.co.za

PROTECTION OF PERSONAL INFORMATION -POPI POLICY AND COMPLIANCE

This practice is committed to compliance with, and adheres to, the protection of the Personal Information Act (POPIA) South Africa, and confirms that we comply with this legislation.

Introduction

The POPI Act requires us to:

1. Sufficiently inform patients (data subjects) of the purpose for which we will process their personal and medical information such as the findings of our initial occupational therapy assessment, progress notes and treatment recommendations communicated to and amongst the clinical team;
2. To collect and process the personal and medical details is a pre-requisite for the therapy intervention and necessary for billing purposes;
3. We capture the details in our practice administration and billing software to submit electronically (secured) to the respective medical aids ;
4. Protect our Information assets from threats, whether internal or external, deliberate or accidental. This policy and compliance framework establishes measures and standards for the protection and lawful processing of personal information within our practice and provides principles regarding the right of individuals to privacy and to reasonable safeguarding of their personal information.

The Information Officer (Inge Steinhoff) is responsible for:

- Conducting a preliminary assessment;
- The development, implementation and monitoring of this policy and compliance framework;
- Ensuring that this policy is supported by appropriate documentation;
- Ensuring that documentation is relevant and kept up to date;
- Ensuring this policy and subsequent updates are communicated to relevant managers, representatives and staff, where applicable.

All employees are responsible for adhering to this policy and for reporting any security breaches or incidents to the Information Officer.

Any service provider that provides information technology services, including data storage facilities, to our practice must adhere to the requirements of the POPI Act to ensure adequate protection of personal information held by them on our behalf. Written confirmation to this effect is obtained from relevant service providers.

Policy Principles

Principle 1: Accountability

- We take reasonable steps to ensure that personal information obtained from patients is stored safely and securely.

Principle 2: Processing limitation

- We collect personal information directly from patients or their appointed family member where it is not possible to obtain the information directly from the patient, due to ill health.
- Once in our possession we will only process or release patient information with their consent except where we are required to do so by law. In the latter case we will always inform the patient.

Principle 3: Specific purpose

- We collect personal information from patients to enable us to treat patients and provide them with appropriate medical care.

Principle 4: Limitation on further processing

- Personal information may not be processed further in a way that is incompatible with the purpose for which the information was collected initially.

Principle 5: Information quality

- We ensure that patient information is complete, up to date and accurate before we use it. This means that it may be necessary to request that patients, from time to time, update their information and confirm that it is still relevant. The responsibility to provide up to date personal information or update the information if changes occurred, lies with the patient.

Principle 6: Transparency/openness

- Where personal information is collected from another source, we are responsible for ensuring that the patient is aware:
 - That their information is being collected;
 - Who is collecting their information by giving them our details;
 - Of the specific reason that you are collecting their information.

Principle 7: Security safeguards

- We ensure technical and organisational measures to secure the integrity of personal information, and guard against the risk of loss, damage or destruction thereof.
- Personal information is also be protected against any unauthorised or unlawful processing.
- We are committed to ensuring that information is only used for legitimate purposes with the patient's consent and only by authorised employees of our practice.
- All devices used for storage of personal and medical information are password/ pass code protected.
- Places where paper files are stored are secured and locked.

Principle 8: Participation of individuals

- Patients are entitled to know particulars of their personal information held by us, as well as the identity of any authorised employees of our practice that had access thereto.
- They are also entitled to correct any information held by us.