	DOCUMENT NAME	DOCUMENT NUMBER
	CONFIDENTIALITY OF HEALTH RECORDS	

VERSION	**1**	
COMPILED BY		**DATE**
AUTHORIZED BY		**07/2025**
NEXT REVISION DATE		**07/2027**

1. PURPOSE & SCOPE

To ensure that all user health records, whether paper-based or electronic, are managed in a manner that protects the privacy of personal health information and complies with Section 14 of the National Health Act and the POPIA (Protection of Personal Information Act).

This SOP applies to all health care personnel, administrative staff, contractors, and any other individuals who have access to health records within the practice.

2. RESPONSIBILITIES

Job description of person responsible	Duties
All Staff:	Must always safeguard health records.
Practice Manager:	Must ensure systems are in place to enforce this SOP and train staff accordingly

3. DEFINITIONS

Health Records: Any information relating to the physical or mental health of a user, recorded by a health care provider.

Confidentiality: The obligation to protect user information from unauthorized access or disclosure.

4. PROCEDURE

All health records must be kept confidential and must not be accessed, discussed, or shared with unauthorized individuals.

Unauthorised access to health records is strictly prohibited and will result in disciplinary action.

Physical Record Management

- Paper records must be stored in a **secure, lockable room** or **filing cabinets** with restricted access.
- During consultations, records must not be left unattended in open areas.
- All records must be returned to the records room **immediately after use**.
- Records awaiting review or audit must be placed in clearly labelled, covered trays in a **restricted access area**.

Electronic Record Management

- All electronic health records must be **password-protected**.
- Access must be **role-based**, with audit logs maintained.
- Computers and tablets must be **locked when unattended**.
- Records accessed offsite must be through a **secure VPN or encrypted platform**.

During User Visits

- Records for users waiting to be seen must be **placed face-down** or **in folders** on the provider's desk.
- Records should never be left exposed in public or semi-public areas.

Clinical Audits and Administrative Use

- Records used for audits or admin must remain in **staff-only** areas.
- These records must be tracked, signed out and signed back in.

Breach Protocol

Any suspected breach of confidentiality must be reported immediately to the Practice Manager, who will initiate an internal investigation in line with the POPIA and National Health Act.

Training

All staff must receive training on this SOP during induction and annually thereafter.

Monitoring & Review

The practice will conduct quarterly checks to verify compliance.
This SOP will be reviewed **every 24 months** or when legislation changes.

5. INTERNAL SUPPORTING DOCUMENTATION

Document	Number	Retention period	Location

6. ATTACHMENT

	DOCUMENT NAME	DOCUMENT NUMBER
	CONFIDENTIALITY OF HEALTH RECORDS	

Receipt Acknowledgement for this SOP

I have read and been informed about the content, requirements, and expectations of this policy for this practice. I understand that if I have questions, at any time, regarding this policy, I will consult with my immediate supervisor or my Human Resources staff members. Please read the policy/procedure carefully to ensure that you understand the policy/procedure before signing this document.

Employee Signature	Employee Printed Name	DATE	Employee Signature	Employee Printed Name	DATE