POPIA Compliance Policy

Dr Lana Bouwer | General Medical Practitioner | Practice Number: PR1029665

1. Policy Statement

Dr Lana Bouwer is committed to protecting the privacy, confidentiality, integrity and availability of all personal information processed by the practice. This policy sets out how the practice collects, uses, stores, shares, secures and destroys personal information in accordance with the Protection of Personal Information Act, 2013 (POPIA), applicable healthcare obligations and sound clinical governance standards.

2. Practice Details

Practice Name	**Dr Lana Bouwer**
Type of Entity	Sole Proprietor
Practice Number	PR1029665
Nature of Business	General Medical Practitioner
Physical Address	160 Kommissaris Street, Welgemoed
Telephone Number	072 170 1016
Email Address	bouwer.lana@gmail.com

3. Purpose of this Policy

The purpose of this policy is to ensure that the practice processes personal information lawfully, transparently and responsibly, particularly patient health information, which is special personal information under POPIA. The policy also provides a practical framework for staff, locums, service providers and any other persons who may handle information on behalf of the practice.

4. Scope

This policy applies to all personal information processed by the practice, including information relating to patients, prospective patients, dependants, parents or guardians, employees, contractors, locums, suppliers, referring practitioners, medical schemes and other third parties. It applies to information processed in paper files, electronic systems, email, messaging platforms, billing systems, appointment systems, backup media and any other storage or communication channel used by the practice.

5. Information Officer

As a sole proprietor, Dr Lana Bouwer is the responsible party for the practice and will act as the Information Officer unless another person is formally appointed in writing. The Information Officer is responsible for overseeing POPIA compliance, responding to patient information requests, managing privacy incidents, maintaining this policy and ensuring that staff and operators understand their privacy obligations.

6. Types of Personal Information Processed

- Patient identification and contact details, including names, identity numbers, dates of birth, addresses, telephone numbers and email addresses.
- Medical and health information, including medical history, diagnoses, treatment notes, prescriptions, referrals, test results, certificates and clinical correspondence.
- Medical aid and billing information, including scheme details, membership numbers, claims information, invoices and payment records.
- Emergency contact, next-of-kin, guardian or dependant information where relevant to treatment or administration.
- Employee, contractor, locum and supplier information necessary for practice administration and legal compliance.

7. Lawful Basis for Processing

The practice processes personal information only where there is a lawful and legitimate basis to do so. This may include processing that is necessary to provide healthcare services, obtain informed consent, manage appointments, maintain clinical records, submit medical aid claims, issue invoices, comply with legal or professional obligations, protect the legitimate interests of the patient or practice, respond to emergencies, or where the patient has given specific consent for a defined purpose.

8. Collection of Personal Information

The practice will collect personal information directly from the patient wherever reasonably possible. Information may also be collected from parents or guardians, referring practitioners, hospitals, laboratories, medical schemes, emergency contacts or other healthcare providers where this is necessary for treatment, administration, continuity of care, billing, claims processing or legal compliance.

9. Use and Disclosure of Personal Information

Personal information will be used and disclosed only for purposes that are lawful, relevant and necessary. This may include providing medical treatment, communicating with patients, maintaining clinical records, referring patients to other healthcare providers, issuing prescriptions or certificates, processing medical aid claims, collecting fees, complying with regulatory requirements, responding to lawful requests and managing the practice.

The practice will not sell patient information or disclose information to unrelated third parties for marketing purposes. Where information must be shared with an operator or external service provider, the practice will take reasonable steps to ensure that the provider protects the information and processes it only on the practice’s instructions.

10. Patient Rights

Patients and other data subjects have the right to be informed about how their personal information is processed, request access to their information, request correction or updating of inaccurate information, object to processing in appropriate circumstances, withdraw consent where processing is based on consent, request deletion where legally permissible, and lodge a complaint with the Information Regulator if they believe their rights have been infringed.

11. Security Safeguards

- Restrict access to patient information to authorised persons who need the information for treatment, administration or practice management.
- Keep physical records in secure areas and avoid leaving patient files or documents unattended.
- Use passwords, access controls and reasonable technical safeguards for electronic systems.
- Use secure backup and recovery processes for important practice information.
- Take reasonable care when sending information by email, messaging platforms or other electronic channels.
- Ensure staff, locums and service providers understand their confidentiality and privacy obligations.
- Dispose of paper and electronic records securely when retention is no longer required.

12. Retention of Records

The practice will retain personal information only for as long as it is required for the purpose for which it was collected, for continuity of care, to comply with legal and professional record-keeping obligations, to manage billing or claims, or to protect the legitimate interests of the patient or practice. When records are no longer required, they will be securely destroyed, deleted, de-identified or archived in accordance with applicable requirements.

13. Operators and Service Providers

Where the practice uses third-party service providers to process personal information on its behalf, such as practice management software providers, billing administrators, IT support providers, cloud storage providers, laboratories, payment providers or document destruction providers, the practice will take reasonable steps to ensure that these providers maintain appropriate confidentiality, security and data protection controls.

14. Data Breach and Incident Management

If the practice becomes aware of unauthorised access, loss, disclosure, alteration or destruction of personal information, the Information Officer will assess the incident, take steps to contain and remediate the risk, document the incident, notify affected persons where required, and report the incident to the Information Regulator where POPIA requires notification.

15. Direct Marketing and Patient Communication

The practice may communicate with patients about appointments, treatment, test results, billing, medical aid claims, recalls, follow-up care and administrative matters. Direct marketing or promotional communication will only be sent where lawful and appropriate, and patients will be given a reasonable opportunity to opt out where required.

16. Cross-Border Transfers

If personal information is stored, accessed or processed outside South Africa, including through cloud-based systems, the practice will take reasonable steps to ensure that the transfer is lawful and that the recipient provides adequate protection for the information, whether through applicable law, contractual commitments or another lawful mechanism recognised under POPIA.

17. Training and Awareness

The practice will ensure that any person who handles personal information on behalf of the practice is made aware of this policy, confidentiality requirements, acceptable use of patient information, secure communication practices and the need to report privacy incidents promptly.

18. Policy Review

This policy will be reviewed at least annually, or sooner if there are material changes to the practice, applicable law, technology, operators, record-keeping processes or information security risks.

19. Approval

Approved by	**Dr Lana Bouwer**
Role	Responsible Party / Information Officer
Signature	
Date	
Next Review Date	