BLOEMENDAL
CLINIC

Klapmuts Simondium Rd
Simondium 7670
T 021 8633399
admin@bloemendalclinic.com
www.bloemendalclinic.com

Bloemendal Addiction Treatment PTY LTD Trading as Bloemendal Clinic

Reg No.: 2012/116357/07

Klapmuts-Simondium Road

Simondium

7670

Email: admin.bloemendalclinic.com

COMPLIANCE MANUAL FOR THE PROTECTION OF PERSONAL INFORMATION ACT OF 2013

BLOEMENDAL CLINIC

Klapmuts Simondium Rd
Simondium 7670
T 021 8633399
admin@bloemendalclinic.com
www.bloemendalclinic.com

CONTENTS:

BLOEMENDAL CLINIC

Klapmuts Simondium Rd
Simondium 7670
T 021 8633399
admin@bloemendalclinic.com
www.bloemendalclinic.com

A. INTRODUCTION

The protection of Personal Information Act (POPIA)is intended to give effect to the constitutional right of privacy for safeguarding personal information by a responsible party and prescribes: -

- Minimum requirements for the lawful processing of personal information,
- An obligation on the Information Officers of public and private bodies to designate or delegate any power of duty to Deputy Information Officers, as necessary to make the body as accessible as possible; and
- Compulsory requirements for registration of Information Officers with the Information Regulator

This Compliance Manual sets out the framework for our company's compliance with POPI and PAIA.

Where reference is made to the "processing" of personal information, this will include any activity in which the information is used, from the time that the information is collected until it is destroyed. "Data" is all the personal information that are collected at the clinic from the patient.

B. PROTECTION OF DATA:

Clinical Patient Records/files of current patients are access controlled as follows:

- Patient records are stored in a locked cabinet in the nurse's station. A nursing staff member always have the keys to the cabinet on her person. All therapist notes must be incorporated into the file that is kept in the Nurses station. No person may access these files without the express permission of the Hospital Manager or Nursing Manager. If a doctor asks for the file, he/she may read it in the Nurses' station and may not leave with it. These files remain the sole responsibility of the Nursing Team.
- The Clinic Administrator manages the administration part of the file from the Administration office.
  When the patient is discharged, the Nursing staff delivers the patient record to the Clinic Administrator, whose duty it is to file the patient records in the archive.

- The Administration record of the patient and the medical record of the same patient are kept in separate files but filed together in the same position. This is to

Klapmuts Simondium Rd
Simondium 7670
T 021 8633399
admin@bloemendalclinic.com
www.bloemendalclinic.com

ensure that the administration record can easily be accessed if needed, without having to access the medical record.

- The Clinic Administrator, nursing staff and clinical staff (doctors, psychologists, and occupational therapist) receive training about the strict controls regarding access and confidentiality of patient records.
- Keys to the archive are kept in the Nurses' Station under control of the Nursing Manager. Another set of keys are kept by the Clinic Administrator. Neither the Nursing Manager nor the Clinic Administrator allows any staff to access the Archive. Access to the archive is therefore restricted.
- Should a patient file be needed by a HPCSA registered staff member, they must request the file from the Clinic Administrator, who will only allow the release of the file to the particular staff member, once the Hospital Manager or Nursing Manager has given permission. That file must be signed out and signed back in. It is not allowed to remove patient records from the clinic premises.
- All staff who work with patient files are required to sign explicit confidentiality agreements. Confidentiality clauses also form part of the employment contracts.
- Electronic patient records, where it applies, conform to the same strict measures. In addition, electronic files are password protected, with each staff member having an individual password to access files.
- All staff are required to have passwords on their computers/ laptops as well as anti-virus software. All staff emails are sent through the protected server of the clinic.

Clinical Patient Records/files (clinical healthcare information):
Of discharged patients are stored in the clinic's Archive which is access controlled as follows:

- Mental Health files are required to be kept for life (until the patient's death), it may not be destroyed.
- The clinic Archive space is Fire-proof and flood proof.
- The archive storage space is fitted with metal cabinets for storage of records.
- The door to the archive room is a fire-proof door and is kept always locked.
- Only staff who are allowed access to the archives are allowed to use it, namely the Nursing Manager, the Registered Nurse on duty, the Hospital Manager, and the Clinic Administrator.
- Patient files are kept on site for as long as the archive space allows, and thereafter will be removed to a warehousing company with strict controls.
- If a patient passes away, it is the responsibility of the clinic to ensure that those records are kept for ten years, before being destroyed.
- Files are archived when the patient has been discharged.

BLOEMENDAL CLINIC

Klapmuts Simondium Rd
Simondium 7670
T 021 8633399
admin@bloemendalclinic.com
www.bloemendalclinic.com

Clinical Patient Records/files (clinical healthcare information):
Preservation of Records

The patient records are physically protected from damage in the following way from environmental risks in the archive:

- The archive has a smoke and fire alarm.
- Chemical fire extinguisher is present.
- The archive has a fire door, fire retardant ceiling and cement floors.
- No sprinkler system for fire is installed in the archive since water can be very damaging to records.
- The door and window in the archive close properly.
- The archive contains metal filing cabinets which lock, and the archive entrance door has a secure safe lock.
- The window in the archive is protected by secure burglar bars.
- The entrance to the archive door is monitored by CCTV.
- The archive doesn't contain plumbing.
- The archive is included in a routine schedule for pest control to prevent insects and rodents damaging records.
- The archive is routinely inspected for any risks such as defective wiring, leaking roof, damp walls, insects, rodents, or any other potential risk.

Electronic records are regularly backed up and the back-up disk is kept at a secure off-site location.

Client/patient information (billing information):
Administration:

- Intake forms (paper) and billing information – administration file of patient, metal locked cabinet in the administration office of clinic, keys kept by the Clinic Administrator only. Billing information are stored with the administration records, and kept until 10 years after the patient's death.
- Electronic – Xpedient software programme – password protected computers only of the clinic administration and another password is required to access the Xpedient software programme.

Client/patient information (accounting information):
Accounts:
Electronic (computer) for processing of monthly salary or consultant fees – pastel software – accounting officer – password protected computer
Electronic (computer) for auditing of clinic accounts – accounting electronic software kept by accountant and auditor – with password protected computers.
Staff and Consultant information:
Employee or Consultant files:

BLOEMENDAL CLINIC
Klapmuts Simondium Rd
Simondium 7670
T 021 8633399
admin@bloemendalclinic.com
www.bloemendalclinic.com

These files are kept in the Human Resources locked metal cupboard. The keys are kept by the directors and Hospital manager, who work with employee related matters. All staff who work with employee records sign confidentiality agreements.

Staff and Consultant information:
Accounts:
Electronic (computer) for processing of monthly salary or consultant fees – pastel software – accounting officer. Computers are password protected and have anti-virus software.
Electronic (computer) for auditing of clinic accounts – accounting electronic software kept by accountant and auditor on password protected computers.

PERIOD RECORDS ARE KEPT AND DESTRUCTION OF RECORDS

Clinical Patient Records/files (clinical healthcare information):

- Mental Health files are required to be kept for life (until the patient's death); it may not be destroyed.
- In the event that a patient passes away, it is the responsibility of the clinic to ensure that those records are kept for ten years, before being destroyed.

Client/patient information (billing information):

Billing information is kept with the administrative information. This means that it is also kept for as long as the patient is alive and 10 years thereafter. Destruction is done by shredding.

Staff and Consultant information:
These are kept until 3 years after last date of employment, according to the Basic Conditions of Employment Act.

All destruction of data is done by shredding.

A Data retention and destruction policy is available on request from the Information Officer.

BLOEMENDAL CLINIC
Klapmuts Simondium Rd
Simondium 7670
T 021 8633399
admin@bloemendalclinic.com
www.bloemendalclinic.com

C. INCIDENT RESPONCE

Should there be any data leaked or misused, we will follow our incident response policy that read as follows:

INCIDENT RESPONSE POLICY

1. Introduction

This policy is developed as the Practice's official incident response policy to deal with information security incidents that may occur in the Practice. As the Practice processes both personal and special personal information, this policy forms an integral part of the Practice's POPI compliance framework.

2. Purpose

This policy sets out the process for handling a security compromise, data breach or any other related incident.

3. Legislation

This policy gives effect to many of our responsibilities as a responsible party in terms of the Protection of Personal Information Act 4 of 2013

4. Applicability of Policy

This policy is applicable to every person employed in the practice or associated with the Practice in any way.

5.Incident

5.1. ***Incidents***. An incident is a security compromise or any other related incident where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person. This definition has three components:

• **reasonable grounds to believe** – an average person would have thought that there was a security compromise from the circumstances.

• **personal information of a data subject** – the security compromise concerned personal information belonging to a data subject; and

Klapmuts Simondium Rd
Simondium 7670
T 021 8633399
admin@bloemendalclinic.com
www.bloemendalclinic.com

• **accessed or acquired by any unauthorised person** – someone who were not supposed to have accessed or acquired the personal information has done so.

Incidents include:

• **loss or theft** – of data containing personal information or equipment on which data containing personal information is stored.

• **hacking** – or any other deliberate attack on our systems to access data containing personal information.

• **access control failure** – a failure of a password, firewall, or other access control system that allows unauthorised access to personal information.

• **unauthorised use** – of personal information by a member of our personnel.

• **equipment failure** – failed equipment that exposes personal information to unauthorised access.

• **human error** – a person making a mistake that exposes personal information to unauthorised access.

• **phishing** – or other ways of using persuasion or guile to obtain personal information without authorisation.

5.2. Impact of Incident

The Practice will establish the nature, extent, and potential consequences of the Incident

• the **severity** of the incident and the consequences to the data subjects involved in the incident

• what **type** of personal information is involved

• what has **happened** to the personal information

• **who** has accessed or acquired the personal information without authorisation

• what is the **extent** of the security compromise or related incident

• who are the **data subjects** whose personal information has been compromised

• what **harm** could come to those data subjects

Klapmuts Simondium Rd
Simondium 7670
T 021 8633399
admin@bloemendalclinic.com
www.bloemendalclinic.com

6. Report

Where an incident comes to the attention of any employee or any other person associated to or affiliated with the Practice, such person must immediately report the incident to the Information Officer.

7. Respond

Any response to a security compromise or related incident will be backed up by a containment and recovery plan that seeks to limit the damage of the incident.

8. Notification.

Information Regulator

Section 22(1)(a) of POPIA and Article 33(1) requires the Information Officer to notify the Information Regulator of any incident without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the breach is unlikely to result in a risk to the rights of the data subjects.

The notification must contain at least:

• a breach description, including

(i) categories and approximate number of data subjects and

(ii) categories and approximate number of personal data records concerned.

• information officer name and contact details.

• likely consequences of the data breach; and

• measures taken or proposed to address the personal data breach and mitigate its possible adverse effects (where appropriate).

Affected Data Subjects

Section 22(1)(b) of POPIA requires notification of the data subjects affected by the incident unless their identity cannot be established. We may only delay notifying the data subjects in terms of section 22(3) of POPIA if a public body responsible for the prevention, detection, or

Klapmuts Simondium Rd
Simondium 7670
T 021 8633399
admin@bloemendalclinic.com
www.bloemendalclinic.com

investigation of offences or the Regulator determines that notification will impede their criminal investigation.

Section 22(4) of POPIA requires the notification to the data subject to be in writing and communicated in at least one of the following ways:

• physically delivered to the data subject's last known physical or postal address.

• electronically delivered to the data subject's last known e-mail address.

• placed in a prominent place on our website.

• published in the news media; or

• as the regulator may direct.

Section 22(5) of POPIA requires the notification to contain enough information to allow the data subject to take steps against the consequences of the compromise, including:

• a description of the possible consequences of the incident.

• a description of the steps that we intend to take to handle the security compromise.

• suggestions of what the data subject could do to mitigate the consequences of the security compromise.

• the identity of the unauthorised person who may have accessed or acquired the personal information (if known to us).

It should also provide advice on how data subjects can mitigate the consequences of the incident and have a mechanism to deal with complaints.

9. Response after an incident.

9.4. *Update policy*.

Update policy to address any deficiencies that were not provided for previously.

9.5. *Update information security*.

The Practice must assess the information security in place and make all necessary improvements to prevent, as far as possible, future Incidents.

Section 19(3) of POPIA and requires the Practice to have due regard to generally accepted information security practices and procedures which may apply to us generally or be required in terms of our industry rules and regulations.

BLOEMENDAL CLINIC

Klapmuts Simondium Rd
Simondium 7670
T 021 8633399
admin@bloemendalclinic.com
www.bloemendalclinic.com

D. Our Information Officer and Deputy Information Officer details:

Information Officer Name: Hester Bothma
Designation: Hospital Manager
Address: Klapmuts-Simondium Road
Simondium
7670
Telephone: (021) 863 3399
Email : h.bothma@bloemendalclinic.com

Deputy Information Officer Name: Jo-dine Jacobs
Designation : Assistant Hospital Administrator
Adress : Klapmuts-Simondium Road
Simondium
7670
Telephone : (021) 863 3399
Email : jodine@bloemendalclinic.com

BLOEMENDAL CLINIC

Klapmuts Simondium Rd
Simondium 7670
T 021 8633399
admin@bloemendalclinic.com
www.bloemendalclinic.com

E. Forms implemented by the Clinic

(Available on request from Information Officer)

- Patients Records Management Policy
- Archiving Policy
- Confidentiality Agreement Form
- Consent to process personal information
- Non-disclosure Agreement for employees
- Privacy notice
- Operator Agreements
- Request for access to record of private Body (Form C Act No.2 of 2000)
- Request for correction or deletion of personal information or destroying or deletion of record of personal information
- Notification of data breach
- Withdrawal of consent.
- Data retention and destruction policy & Schedule
- Incident Response policy
- Training of staff
- Different Forms used in clinic that shows our compliance