DR MARINUS
APPELGRYN-SIEBERT

GENERAL PRACTITIONER
OCCUPATIONAL MEDICAL PRACTITIONER
M.B.CH.B (PRET) DOMH

POPI & PAIA MANUAL

FOR THE IMPLEMENTATION OF THE

PROTECTION OF PERSONAL INFORMATION ACT NO. 4 OF 2013

&

FOR THE APPLICATION OF THE

PROMOTION OF ACCESS TO INFORMATION ACT NO. 2 OF 2000 (as amended)

TABLE OF CONTENTS

Approval:

Name	Position	Signature	Date
Version 1	**01 AUGUST 2025**		

SCOPE OF THE MANUAL

This manual applies to the practice of **DR MARINUS APPELGRYN-SIEBERT INC.**

COMPANY CONTACT DETAILS

The scope of the manual is limited to the records held by

The Company: **DR MARINUS APPELGRYN-SIEBERT INC.**
Registration number: 2020/622288/21
Registered address: 1st Floor, Langebaan Med Centre, 1 Rosemary Avenue, Mykonos, Langebaan, 7357

Website address: https://www.drmarinus.co.za/
Tel: 022 634 0003
Email: reception@drmarinus.co.za

The Information Officer: **DR MARINUS APPELGRYN-SIEBERT**

Email: dr@drmarinus.co.za
Contact numbers: 022 634 0003

---

1. PURPOSE OF THIS MANUAL

The Protection of Personal Information Act 4 of 2013 (POPIA) and the Promotion of Access to Personal Information Act 2 of 2000 (PAIA), gives effect to Section 32 of the Constitution's right of privacy and looks at two opposing interests relating to that of personal information, from an individual point of view and access to personal information for the legitimate purpose of conducting business.

POPIA provides guiding principles to promote the protection of privacy which are intended to be applied to the processes of personal information accessibility and sharing.

PAIA gives legislative effect to person's right of access to information and accountability for both private and public bodies who has a duty to provide to a requester of records, unless specifically refused in terms of Section 11 of PAIA. It's designed to empower people to use the law and empower themselves so as to facilitate the requesting of access of information in different ways.

The purpose of this manual as set out below is to protect **DR MARINUS APPELGRYN-SIEBERT INC.** and to inform stakeholders and data subjects of the compliance associated with the protection of, and the right to access, Personal Information which includes:

- breaches of confidentiality;
- failing to offer choice; and
- reputational damage;

DR MARINUS APPELGRYN-SIEBERT INC. will ensure that the highest standard of compliance with policies, regulations, and laws to protect Personal Information is maintained at all times.

2. AVAILABILITY OF THIS MANUAL

a. This PAIA and POPI Manual is available for inspection during office hours from the Information Officer, free of charge.
b. Additionally, this PAIA and POPI Manual can be viewed on the Company website at: https://www.drmarinus.co.za/

3. GENERAL DEFINITIONS

Access	The right, the opportunity, or the means of finding, using, or retrieving information.
Accountability	The condition that individuals, organisations, and the community are responsible for their actions and may be required to explain them to others.
Anonymous information	Information which does not relate to an identified or identifiable natural person or to personal information rendered anonymous in such a manner that the data subject is not or no longer identifiable.
Anti-malware	Software built to detect and block malware from infecting computers and devices.
Anti-virus	Software developed to identify and eliminate computer viruses.
Automated	Decisions made by machine (computers), without human intervention. For example, to automatically accept or deny an online credit application or the automated processing of CVs that evaluates (profiles) personal aspects of individuals to determine if they will qualify for a position.
Classification	The process of assigning an appropriate level of classification to an information asset to ensure it receives an adequate level of protection.
Cloud Storage	A method of saving digital data, like documents on remote servers that are accessed via the internet. Instead of storing files on a local device or physical hard drive, users upload them to servers managed by third-party providers, allowing access from anywhere with an internet connection.
Confidentiality	Is managed by the set of rules that limits access to information.
Consent	Of the data subject means, any voluntary, specific, and informed expression of will in terms of which permission is given for the processing of personal information.
Data subject	The person to whom personal information relates.

Encryption	The process of converting information or data into a code, especially to prevent unauthorised access.
Filing system	Any structured set of personal information which are accessible according to specific criteria, whether centralised, decentralised, or dispersed on a functional or geographical basis.
Information Regulator	The **Information Regulator of South Africa** is an independent authority established under Section 39 of the *Protection of Personal Information Act* (POPIA) of 2013. It operates autonomously, accountable only to the law, the Constitution, and the National Assembly.
Integrity	The assurance that information is trustworthy and accurate.
Operators	A natural or legal person, public authority, agency or other body which processes personal information on behalf of the Responsible Party. When dealing with an operator, it is considered good practice for a responsible party to include an indemnity clause.
Personal information	Information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person such as a company, including, but not limited to. Refer Section 6 of this document for a full definition.
Policies	Clear and measurable statements of preferred direction and behaviour to condition the decisions made within an organisation.
Policy	Clear and measurable statements of preferred direction and behaviour to condition the decisions made within an organisation.
Private Body	Under the *Promotion of Access to Information Act* (PAIA) as: • A **natural person** who carries or has carried on any trade, business, or profession (in that capacity) • A **partnership** engaged in trade, business, or profession • A **juristic person**, whether existing or former (e.g., companies, NGOs) • A **political party** It specifically **excludes public bodies**, which are government departments or entities exercising public powers.

Process	A set of interrelated or interacting activities that transforms inputs into outputs.
Processing	Any operation or set of operations which is performed on personal information or on sets of personal information, whether or not by automated means, such as; collection, recording, organisation, collating, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Public Body	Any department of state, administration in the National or Provincial sphere of government or any Municipality in the local sphere of government.
Reconstruction	Refers to the process of reproducing or restoring lost, damaged, or destroyed records using available information, secondary evidence, or copies. This can be done manually or digitally.
Record	Means any recorded information, regardless of its medium or form, including: • Writing on any material; • Information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored; • Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means; • Book, map, plan, graph or drawing; • Photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced.
Responsible Party	The responsible party is the entity that needs the personal information for a particular reason and determines the purpose of and means for processing the personal information. In this case, the organisation is the responsible party.
Restriction	To withhold from circulation, use or publication any personal information that forms part of a filing system, but not to delete or destroy such information - for example - temporarily moving the data to another processing system, making the data unavailable to users, or temporarily removing published data from a website.

Risk	A threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided or mitigated through pre-emptive action.
Safeguards	The protections or measures put in place to prevent harm, danger, or unwanted outcomes.
Security compromise	A security compromise means a security compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal information transmitted, stored or otherwise processed.
Special information	Personal information including religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, criminal, health or sex life or biometric information.
The Company	DR MARINUS APPELGRYN-SIEBERT INC. registered within the Republic of South Africa with Registration Number: 2020/622288/21
The Information Officer	Is responsible for ensuring the organisation's compliance with the POPI Act and is registered with the Information Regulator. The Information Officer ensures compliance with POPIA and promotes a culture of privacy and data protection throughout the organisation.
The Regulator	The Information Regulator established in terms of section 39 of POPIA

4. LEGISLATION

Records are held in accordance with but not limited to the following legislation:

Basic Conditions of Employment Act 75, 1997

Children's Act 38, 2005

Choice of Termination of Pregnancy Act 92, 1996

Companies Act 71, 2008 (as amended)

Competition Act 89, 1998

Compensation for Occupational Injuries and Diseases Act 130, 1993

Constitution of the Republic of South Africa, 1996

Consumer Protection Act 68, 2008

Debt Collectors Act 114, 1998

Electronic Communication and Transactions 25, 2002

Employment Equity Act 55, 1998

Financial Intelligence Centre Act 38, 2001

Health Professions Act 56, 1974

Income Tax Act 58, 1962

Labour Relations Act 66, 1995

Magistrates Court Act 32, 1944 (Garnishee and Administration orders)

Medical Schemes Act 131 of 1998

Medicines and Related Substance Act 101 of 1965

Mental Health Care Act 17 of 2002

National Credit Act 34, 2005

National Health Act 61 of 2003

National Health Laboratory Services Act 37 of 2000

Occupational Health and Safety Act 85, 1993

Skills Development Act 97, 1998

Skills Development Levies Act 9,1999

South African Revenue Service Act 34, 1997

Taxation Laws Amendment Act 34, 2019

The Law of Contract, Common Law

Unemployment Insurance Act 63, 2001

Unemployment Insurance Contributions Act 4, 2002

Value-Added Tax Act 89, 1991

The above list is not a comprehensive list and does not include all relevant laws within the borders of South Africa.

5. THE INFORMATION OFFICER FUNCTION

Once appointed, the Information Officer must be registered with the South African Information Regulator established under POPIA prior to performing his or her duties. Deputy Information Officers can also be appointed to assist the Information Officer.

Where no Information Officer is appointed, the head of the organisation will be responsible for performing the Information Officer's duties as contemplated in section 1 of the Promotion of Access to Information Act or in relation to a public body means an information officer or deputy information officer as contemplated in terms of sections 1 or 17 of the Promotion of Access to Information Act.

The primary responsibility of the Information Officer is to promote adherence to the Protection of Personal Information Act (POPIA) across the organisation, fostering a culture where privacy and data protection are embedded in decision-making at every level. This role involves safeguarding all personal data held by the company through a combination of robust physical security and the implementation of industry best practices. Before assuming any responsibilities, the Information Officer must be formally registered with the regulatory authority.

These responsibilities rely on input and collaboration from various internal departments, such as IT, Finance, and others, as the duties are closely interconnected with the information provided across the organisation.

5.1 Other Responsibilities of an Information Officer:

- Dealing with requests made to the organisation relative to PAIA.
- Cooperation with the Information Regulator relating to any inquiries.
- Maintaining this Compliance Manual and having it available.
- Establishing internal protocols in conjunction with efficient systems designed to manage and respond to requests for information or access appropriately.
- Keeping the Board of Directors up to date about information protection responsibilities and any security breaches.
- Ensuring revision of existing policies to ensure alignment with POPIA requirements and data protection standards.
- Ensuring staff's awareness of all POPIA and PAIA requirements.
- Remaining up to date with any important changes to legislation, and
- That copies of the manual are provided to persons at their request. Hard copies to be provided upon payment of a fee (predetermined by the Information Regulator) as per Form 3 of the Information Regulator.

5.2 Documentation held by the Information Officer

- All risks, incidents, and threats.
- All responses to risks, incidents, and threats.
- Details of all breaches, i.e., time, place, format of data, size of breach, reasons, and possible consequences, etc.
- An action plan to remedy any breach, with the roles and responsibilities of all parties related to the matter.
- Forms and written procedures for all steps related to the stages of any known breaches.

5.2.1 The following information is recorded and managed by the Information Officer.

- An inventory of all data subjects and their personal information.
- Data subject consents and instructions.
- The identities of the data processors.
- How access control is addressed.
- Copies of any communication sent to clients with regard to the POPIA and PAIA acts will be held by the Information Officer.

6. WHAT PERSONAL INFORMATION CAN BE COLLECTED?

POPIA's scope includes both individuals and juristic persons — such as businesses, companies, and other legally recognised entities. These organisations are treated as data subjects under the law and are granted equal rights to the protection and lawful handling of their personal information.

The definition of Personal Information as stated in the POPI Act is:

*"**personal information** means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to:*

1. *information relating to the race, gender, sex, pregnancy, marital status, family details, nationality, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;*
2. *information relating to the education or the medical, financial, trade union memberships, criminal or employment history of the person;*

3. *any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;*
4. *the biometric information, visual images of individuals captured on CCTV of the person;*
5. *the personal opinions, views or preferences of the person;*
6. *correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;*
7. *the views or opinions of another individual about the person; and*
8. *the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information* about the person;"

6.1 Personal information Categories include:

This information includes but are not limited to name, surname, id number, address, contact details, details of qualifications, tax information, employment history, level of remuneration, date of birth, marital status, race, disability information, background and criminal checks, health and safety records, employee performance records, educational background, CCTV records, income tax reference numbers, electronic access records, training records, invoices, contractual agreements and statutory reporting.

a. Employee Information (Human Resources and Staff Administration)
b. Patient Records
c. Suppliers/Vendors & Contractors Records
d. Marketing and Sales, including all social media
e. Financial and Tax Records
f. Shareholders/Affiliate Companies and Subsidiaries
g. Statutory Records (MOI, Register of Directors, etc.)
h. Health and Safety
i. Banking Institutions and FICA records

The company do not collect special information about our stakeholders, personnel and clients such as religion, health, political beliefs or sexual orientation.

Records of personal information may be retained for periods in excess of the period for which the information was used for historical, statistical or research purposes with appropriate safeguards against the records being used for any other purposes.

7. HOW IS PERSONAL INFORMATION COLLECTED?

When personal information is stored, accessed, or shared within the organisation, we know that there is a duty to ensure its protection through appropriate safeguards and responsible practices.

POPIA applies to personal information processed by or for a responsible party using **automated or non-automated means**.

- For **non-automated processing** (like paper records, photos, x-rays), the Act only applies if the information is part of—or intended to be part of—a **filing system**.
- The Act applies if the **responsible party is domiciled in South Africa**.
- It also applies to **non-domiciled responsible parties** who process personal information using automated or non-automated means **within South Africa**, unless the processing is **solely for forwarding** the information.

The company information is hosted by external service providers, and all the information is stored on the cloud. The information may include, but are not limited to Metadata, IP addresses, contact information,

names, web page access and other data generated through the websites and other categories listed under Section 6.

External hosting providers are engaged to support contractual obligations with both prospective and current patients, ensuring our online services are delivered securely, efficiently, and promptly through a trusted professional partner. These providers will process personal data solely to the extent required to meet their operational responsibilities and in strict accordance with our instructions. Disclosure of personal information to third parties will occur only when necessary for business operations and will not be used for marketing or credit reporting purposes.

THE COMPANY COLLECT PERSONAL INFORMATION THROUGH THE FOLLOWING METHODS:

1. **From the data subject self:**
    a. By contacting the rooms, making an appointment and creating an account.
    b. Email correspondence.
    c. Job Applications.
    d. Website browsing, online cookies.
    e. Biometrics.

8. WHERE IS PERSONAL INFORMATION ACCESSED, PROCESSED AND SHARED?

This section outlines the points at which personal information is accessed and utilised, specifically in relation to the activities carried out by the company, its personnel, clients, and associated third-party stakeholders.

Disclosure of personal information entails the processing of a data subject's information, only for the sole purpose for which the information was collected in order for the company to be able to do its work.

Processing can be defined as the collection, recording, collation, storage, retrieval and alteration, which could include the processing of recorded material, e.g. video or photos taken during an event.

8.1 INTERNAL DOCUMENTATION

Registers and documents pertaining to transactions relevant to personal information:

a. Employee Information Records and Correspondence including permanent, temporary, part-time staff and contractors
b. Employee Agreements / registers
c. Employment Applications (including criminal background checks)
d. Records provided by a third party relating to employees
e. Client Records including client medical history and Medical Aid records
f. Health and Safety (OHASA)
g. Annual Financial Statements
h. Annual Reports
i. Accounting Records
j. Management Statements
k. Bank Records and FICA documents
l. Email Correspondence
m. Statutory Records (MOI, Register of Directors, etc.)
n. Asset registers
o. Rental Agreements
p. Tax Records
q. Loan Agreements

r. Marketing and Sales, including all social media and other publications
s. Clinical Reports including those from other treating physicians
t. Radiology Reports
u. Pathology Reports

8.2 SOFTWARE ON COMPANY OWNED DEVICES AND USED FOR BUSINESS PURPOSES

a. Electronic Health Records.
b. Accounting Software.
c. Inventory Management and POS Systems.
d. Payroll and other HR Software.
e. Antivirus and Malware Software on end-user machines.
f. Antivirus and Malware Software on Network.
g. Marketing Automation Software.
h. Website Analytics Tools.

8.3 THIRD PARTY STAKEHOLDERS – INTERNAL RELATED

3rd Party access and processing include but are not limited to:

The Company identified third-party stakeholders who may have an interest in the personal information held by the Practice.

These include but are not limited to:

a. Agents or distributors of pharmaceutical and medical device products
b. Banking Institutions
c. Patients
d. Attorney/Lawyer
e. Life Insurance Broker
f. Company Secretarial Services Company
g. Employee Unions e.g., labour unions, trade unions, etc.
h. Employees
i. External Accountants
j. HR and Payroll Service Providers
k. Short Term Insurance Company
l. Subcontractors to the Company
m. Tax consultants for Company
n. Security Software Company

8.4 THIRD PARTY INSTITUTIONS – EXTERNAL RELATED

Third-party entities potentially engaged with the company for legislative adherence and official registration processes.

8.4.1 Government Institutions:

CIPC - Company and Intellectual Property Commission
DHA - Department of Home Affairs
DOH - Department of Labour
DTI - Department of Trade and Industry supplier database
Master - Master of the High Court (Johannesburg, Pretoria, Cape Town, etc.)
NCRA – National Credit Reporting Agencies (Equifax, Experian and TransUnion)
SAPS – South African Police Services
SARS - South African Revenue Services
SAQA – South African Qualifications Authority

8.4.2 External Institutions (statutory and non-statutory)

STATUTORY:

AHPCSA	Allied Health Professions Council of South Africa
FIC	Financial Intelligence Centre
HPCSA	Health Professions Council of South Africa
SAPC	South African Pharmacy Council

NON-STATUTORY:

IoSH (SA)	Institute of Occupational Safety and Health SA
SAHPRA	South African Health Products Regulatory Authority
HPCSA	Health Professions Council of South Africa
DSSA	Dermatological Society of South Africa
AAMSSA	Aesthetic and Anti-Aging Medicine Society

All the above parties mentioned under section 8.2, 8.3 and 8.4 will act on behalf of the **Company**, who determines the purpose and means of processing, and must follow the instructions given by the Company.

9. TRANSBORDER ACTIVITY

The Company does not effect any cross-border transfer of personal information for the purpose of facilitating the provision of services. This may include third party suppliers or service providers who perform services on the company's behalf, including cloud storage.

In undertaking such transfers, the Company shall implement all requisite measures to ensure that service providers and third-party operators are subject to applicable legislation, enforceable corporate rules, or binding legal instruments which afford an adequate level of data protection.

10. OWNER CONSENT AND PERSONAL INFORMATION

POPIA sets out a regulatory framework designed to ensure that personal data is processed in a lawful, transparent, and secure manner, upholding the privacy and dignity of individuals and organisations.

POPIA affirms data privacy as a fundamental right and establishes accountability measures that give Data Subjects control over the use of their personal information.

The owner of information is the data subject.

All other relevant parties are considered processors. POPIA requires Data Subjects to direct how their personal information is collected, used, and disposed of.

The data subject remains the owner of its personal information.

The classification of collection of information directly from a data subject or other as stated in the POPI Act is:

> ***12. (1) Personal information*** *must be collected directly from the data subject, except as otherwise provided for in subsection (2)*
>
> *(2) It is not necessary to comply with subsection (1) if -*

a) *information is contained in or derived from a public record or has deliberately been made public by the data subject;*
b) *the data subject or a competent person where the data subject is a child has consented to the collection of the information from another source;*
c) *collection of the information from another source would not prejudice a legitimate interest of the data subject;*
d) *collection of the information from another source is necessary –*
    i. *to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;*
    ii. *to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act, 1997 (Act No. 34 of 1997);*
    iii. *for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated;*
    iv. *in the interests of national security;*
    v. *to maintain the legitimate interests of the responsible party or of a third party to whom the information is supplied;*
e) *compliance would prejudice a lawful purpose of the collection; or*
f) *compliance is not reasonably practicable in the circumstances of the particular case.*

11. RIGHTS OF THE DATA SUBJECT

A Data Subject has the legal right to ensure that their personal information is processed in accordance with the conditions and principles set out in applicable data protection legislation.

1) **The right to access personal information.**
   The data subject has the right to know what personal data is held by the company and can request to access that data.

2) **The right to have personal data corrected or removed.**
   The data subject may request that information held be corrected, updated or removed.

3) **The right to object to processing of personal information.**
   On reasonable grounds, the data subject can object to the processing of their information.

4) **The right to complain to the Information Regulator.**
   If a Data Subject believes POPIA has been violated, they may file a complaint with the Information Regulator for adjudication.

5) **The right to be informed.**
   Data Subjects must be informed when their personal information is collected, particularly in cases of unlawful access.

Should the client's consent be required to process their personal information the client has the right to withdraw their consent.

12. DATA SECURITY SAFEGUARDS

The POPI Act requires companies to protect personal information through reasonable technical and organisational safeguards that prevent unauthorised access or processing.

POPIA applies to personal information stored in both physical (hard copy) and electronic (soft copy) formats. The company must ensure that its IT infrastructure aligns with POPIA's data protection standards, with support from its IT administrator or consultant to address relevant security measures.

Under POPIA, personal information must not be retained longer than necessary for the purpose for which it was collected or processed—unless its continued retention is legally required or authorised, needed by the responsible party for lawful business functions, or consented to by the data subject.

Furthermore, in terms of POPIA, once Personal Information records are no longer required, then such records must be destroyed or deleted as soon as reasonably and practically possible, which destruction or deletion must be done in a manner that prevents its reconstruction into an intelligible form.

12.1 SECURITY SAFEGUARDS WITHIN THE PRACTICE

External hosts implement a range of electronic security features to mitigate risks under POPIA, including firewalls, intrusion detection systems, encryption protocols, secure access controls, and regular vulnerability assessments. These measures help safeguard personal information from unauthorized access, data breaches, and other cyber threats, ensuring compliance with the Act's data protection requirements.

12.1.1 DECOMMISSIONING OF HARDWARE (LAPTOPS, SERVERS, etc)

The decommissioning of a laptop involves the secure removal of all data and the systematic preparation of the device for disposal or repurposing. This process typically encompasses data backup, comprehensive hard drive sanitization, detachment of peripheral components, and adherence to appropriate protocols for environmentally responsible recycling or disposal.

The company takes all practicable measures to ensure that data is comprehensively erased from devices, thereby mitigating the risk of accidental or unauthorized recovery.

12.1.2 HARD COPY (NON-ELECTRONIC) SAFEGUARDS WITHIN THE PRACTICE

The practice stores hard copies of statutory documents in compliance with legislation and internal policies. Archived records are securely kept off-site under fire-proof conditions, with access restricted to authorised personnel. Physical records are locked and protected by practical security barriers.

13. SECURITY BREACHES AND INCIDENT MANAGEMENT

In an event where personal information of a data subject is compromised and accessed unlawfully the practice will take responsibility to notify the Information Regulator as well as the affected parties as soon as reasonably possible. However, the Act allows for delayed notification of the data subject if the Information Regulator or a public body responsible for crime prevention or investigation believes that such disclosure would hinder an ongoing investigation.

13.1 INCIDENT MANAGEMENT POLICY

The Practice has established procedures to manage POPIA-related incidents, with clearly defined roles for data processors and departmental heads who oversee personal data security. Measures are in place to minimize incidents and ensure swift response. Operators are required to promptly report breaches, except where Section 22 of the POPIA applies, both the responsible party and the Regulator will be notified immediately of any security compromise.

13.2 SECURITY BREACHES

The practice's data breach response plan ensures swift, coordinated action among all involved parties, with strict communication protocols. Upon confirmation, the Information Officer is responsible for notifying affected data subjects, the Information Regulator, and other impacted parties, in accordance with POPIA.

13.3 RECORDS KEPT BY INFORMATION OFFICER

The Information Officer maintains records of all risks, incidents, and threats, along with corresponding responses and detailed breach information, including timing, location, data format, breach size, causes, and potential consequences.

13.4 DISCIPLINARY ACTION

The practice has identified procedures to manage incidents that may have an impact on the POPI Act.

Following an investigation, immediate actions may include reporting to law enforcement for possible criminal charges, initiating disciplinary proceedings, and recovering funds or assets to minimize harm or loss.

After investigating an infringement or complaint, the practice may propose suitable administrative, legal, or disciplinary action against any employee reasonably suspected of involvement in non-compliant conduct as described in this manual.

Wilful mishandling or gross negligence in managing personal information will be treated as serious misconduct, and may result in summary **dismissal**. Disciplinary action will be initiated if sufficient evidence supports such non-compliance by an employee.

14. NON-DISCLAIMER

Notwithstanding the provisions of this manual, the Practice shall not be held liable for matters beyond its reasonable control, including but not limited to acts of state, acts of God, instances where the requester is at fault, exemptions granted by the Regulator, or circumstances in which compliance was not reasonably practicable.

15. DESTRUCTION OF DOCUMENTS

As per the Act, the destruction or deletion of a record of personal information must be done in a manner that prevents its reconstruction in an intelligible form.

Records and documents shall be destroyed only upon the expiry of the applicable statutory retention periods and following a determination as to whether such information is required for any other lawful or operational purposes. POPIA permits the retention of personal information beyond the prescribed period when required

by law or for purposes such as historical, statistical, or research use, provided that the responsible party has implemented adequate safeguards to prevent the information from being used for any other purpose.

The practice is responsible for dealing with the destruction of its documents, which must be done on a regular basis. Files must be checked to make sure that they may be destroyed and also to ascertain if there are important original documents in the file.

16. PROCEDURE FOR REQUESTING ACCESS TO INFORMATION

16.1 COMPLETION OF ACCESS REQUEST FORM

In order to facilitate a timely response to requests for access, all requesters should be aware of the following when completing the Access Request Form:

a. Form 2, Access **Request Form** must be completed.
b. **Proof of identity** is required to authenticate the identity of the requester. Therefore, in addition to the access form, requestors will be required to supply a copy of their identification document.
c. Complete the form in BLOCK LETTERS and answer every question.
d. If a question does not apply state N/A in response to that question.
e. If there is nothing to disclose in reply to a particular question state "nil" in response to that question.
f. If there is insufficient space on a printed form, additional information may be provided on an attached referenced folio.
g. When the use of an attached folio is required, precede each answer with the applicable title of that page.

16.2 SUBMISSION OF THE ACCESS REQUEST FORM

The complete Access Request Form together with a copy of the identity document must be hand delivered or submitted either via e-mail and must be addressed to the contact person as indicated above.

This fee is not applicable to personal requesters referring to any person seeking to access records that contain their personal information.

An initial, request fee of R140.00 (including VAT) is payable on submission. Refer to Form 3 under Fees for breakdown of fees.

16.3 PAYMENT OF FEES

Payment details can be obtained from the Information Officer. If the request for access is successful an access fee may be required for the search, reproduction and/or preparation of the record(s) and will be calculated based on the Prescribed Fees.

Proof of payment must be supplied, and the access fee must be paid prior to access being given to the requested record.

If a deposit has been paid in respect of a request for access which is refused, then the Information Officer will refund the deposit to the requestor.

16.4 NOTIFICATION

The practice has leeway of 30 days from receipt of the request to decide whether to grant or decline the request and give notice with reasons to that effect.

The 30-day period within which the practice must decide whether to grant or refuse the request, may be extended for a further period of not more than thirty days, if the request is for a large volume of information and the information cannot be reasonably obtained within the original 30-day period. The practice will notify the requester in writing should an extension be needed.

16.5 COMPLAINTS TO THE INFORMATION REGULATOR

A requester may approach the Information Regulator to lodge a complaint in accordance with Section 77(a) of PAIA on a prescribed form and the form can be sent by email to: PAIAComplaints@inforegulator.org.za

A requester or third party may only lodge a complaint with the Regulator once all internal appeal processes against a decision by the Information Officer or head of a private body have been exhausted.

17. REFUSAL OF ACCESS TO RECORDS

The Practice does not provide for internal appeal procedures in respect of PAIA requests. Accordingly, any decision rendered by the duly authorised individual shall be deemed final.

In the event that a request is refused, the requester has the right to seek recourse by applying to a court of competent jurisdiction.

The main grounds for refusal of a request for information are set out below:

- Mandatory protection of a third party's privacy, where disclosing their personal information would be considered unreasonable.
- Mandatory protection of the commercial information of a third party, if the record contains:
    - Trade secrets;
    - Sensitive financial, commercial, scientific, or technical information that may harm a party's interests if disclosed;
    - Confidential third-party information that could harm their negotiating or competitive position if disclosed.
- Mandatory safeguarding of third-party confidential information when such protection is required under an existing agreement.
- Mandatory protection of the safety of individuals and the protection of property.
- Mandatory protection of records which could be regarded as privileged in legal proceedings.

UNLAWFUL DENIAL OF ACCESS

Where records are required for litigation, or where litigation is reasonably anticipated, all relevant records and documents that may reasonably be subject to discovery or hold relevance to the legal matter must be retained even if the retention period has expired.

In the event of a request for access to records or documents under PAIA, such records and documents must be retained until the PAIA process has been fully concluded. It is essential to note that any individual who unlawfully denies access to requested records, or who intentionally destroys, damages, alters, or falsifies such records, commits an offence and, upon conviction, is liable to a fine or imprisonment for a period not exceeding two years.

18. RECORDS AVAILABLE WITHOUT REQUEST

In accordance with Section 51(1)(d) of the Act, records that are publicly available, such as those published on the practice's website, contained in marketing and promotional materials, brochures, or annual reports, may be accessed without the submission of a formal application.

Other non-confidential records, such as statutory records maintained at CIPC, may also be accessed without the need to submit a formal application, excluding shareholding and UBO (Ultimate Beneficial Ownership) information submitted to CIPC.

19. RECORDS ONLY AVAILABLE UPON REQUEST

In terms of the PAIA Act, Section 51(1)(d) the following records held by the Practice can only be accessed upon the submission of a formal application.

Please note that submitting a completed access request form does not guarantee access to the requested record and it may also be restricted if it falls within specific categories outlined in Chapter 4 of the Act as grounds for refusal.

This serves as a reference but are not limited to the categories of information that the Practice may hold.

Records not listed as automatically available in the PAIA manual of the Practice:

- **Internal correspondence** or communications that are not publicly disclosed;
- **Personal information** of individuals, unless the requester is the data subject or has legal grounds;
- **Confidential commercial information** of third parties;
- **Information protected by agreements**, such as Patient Information and Consent forms or service contracts;
- **Records required for the exercise or protection of rights**, which must be justified in the request;
- **Documents subject to legal privilege**, unless disclosure is mandated by law.

20. INFORMATION REGULATOR'S GUIDE

The Regulator Guide, published by the Information Regulator, helps individuals understand and apply the provisions of PAIA as outlined in Section 14 of PAIA.

The Regulator Guide helps people understand PAIA, lists the types of information they can request, and explains how to make a request.

20.1 The **Regulator Guide** is available in each of the official languages and in braille.

20.2 The **Regulator Guide** contains the description of-

20.2.1 the objects of PAIA;

20.2.2 the postal and street address, phone and fax number and, if available, electronic mail address of-

20.2.2.1 the Information Officer of every public body, and

20.2.2.2 every Deputy Information Officer of every public and private body designated in terms of section 17(1) of PAIA;

20.2.3 the manner and form of a request for-

20.2.3.1 access to a record of a public body contemplated in section 11; and

20.2.3.2 access to a record of a private body contemplated in section 50[1];

20.2.4 the assistance available from the Regulator in terms of PAIA;

20.2.5 all remedies in law available regarding an act or failure to act in respect of a right or duty imposed by PAIA, including the manner of lodging-

20.2.5.1 an internal appeal;

20.2.5.2 a complaint to the Regulator; and

20.2.5.3 an application with a court against a decision by the information officer of a public body, a decision on internal appeal or a decision by the Regulator or a decision of the head of a private body;

20.2.5.4 the provisions of sections 14[2] and 51[3] requiring a public body and private body, respectively, to compile a manual, and how to obtain access to a manual;

20.2.6 the provisions of sections 15[4] and 52[5] providing for the voluntary disclosure of categories of records by a public body and private body, respectively;

---

[1] *Section 50(1) of PAIA- A requester must be given access to any record of a private body if-*

a) that record is required for the exercise or protection of any rights;

b) that person complies with the procedural requirements in PAIA relating to a request for access to that record; and

c) access to that record is not refused in terms of any ground for refusal contemplated in Chapter 4 of this Part.

[2] *Section 14(1) of PAIA- The information officer of a public body must, in at least three official languages, make available a manual containing information listed in paragraph 4 above.*

[3] *Section 51(1) of PAIA- The head of a private body must make available a manual containing the description of the information listed in paragraph 4 above.*

[4] *Section 15(1) of PAIA- The information officer of a public body, must make available in the prescribed manner a description of the categories of records of the public body that are automatically available without a person having to request access*

[5] *Section 52(1) of PAIA- The head of a private body may, on a voluntary basis, make available in the prescribed manner a description of the categories of records of the private body that are automatically available without a person having to request access*

20.2.7 the notices issued in terms of sections 226 and 547 regarding fees to be paid in relation to requests for access; and

20.2.8 the regulations made in terms of section 92[8].

20.3 Members of the public can inspect or make copies of the **Regulator Guide** from the offices of the public and private bodies, including the office of the Regulator, during normal working hours.

20.4 The **Regulator Guide** can also be obtained-

20.4.1 upon request to the Information Officer;

20.4.2 from the website of the Regulator https://www. https://inforegulator.org.za/paia-guidelines/

A copy of the PAIA Guide is available for inspection at the offices of the Information Regulator.

Contact details are as follows:

Address:	Woodmead North Office Park, 54 Maxwell Drive, Woodmead, Johannesburg, Gauteng, South Africa, 2191
Telephone:	010 023 5200
Website:	inforegulator.org.za
E-mail:	enquiries@inforegulator.org.za

[6] *Section 22(1) of PAIA- The information officer of a public body to whom a request for access is made, must by notice require the requester to pay the prescribed request fee (if any), before further processing the request.*

[7] *Section 54(1) of PAIA- The head of a private body to whom a request for access is made must by notice require the requester to pay the prescribed request fee (if any), before further processing the request.*

[8] *Section 92(1) of PAIA provides that –"The Minister may, by notice in the Gazette, make regulations regarding-*

(a) any matter which is required or permitted by this Act to be prescribed;

(b) any matter relating to the fees contemplated in sections 22 and 54;

(c) any notice required by this Act;

(d) uniform criteria to be applied by the information officer of a public body when deciding which categories of records are to be made available in terms of section 15; and

(e) any administrative or procedural matter necessary to give effect to the provisions of this Act."

21. REQUEST FOR INFORMATION DETAILS

Access to the Company's records is granted only after all applicable access requirements have been satisfied.

A requester refers to any individual seeking access to the Company's records who must adhere to the procedures outlined in the Promotion of Access to Information Act (PAIA) when submitting a request.

Refer to the Information Regulator's Prescribed Forms.

Form 2: Request for Access to Record

Form 3: Outcome of Request and Fees Payable

Requests can be submitted either via post, or e-mail and should be addressed to the relevant contact person as indicated below:

Contact person	DR MARINUS APPELGRYN-SIEBERT
Postal Address	POSTNET SUITE 004, PRIVATE BAG X6, LANGEBAAN, 7357
Physical Address	1ST FLOOR LANGEBAAN MED CENTRE, 1 ROSEMARY AVENUE, MYKONOS, LANGEBAAN, 7357
Phone number	022 634 0003
E-mail	dr@drmarinus.co.za