



Dr. Mariska Carter
CLINICAL PSYCHOLOGIST / KLINIESE SIELKUNDIGE

MSc Clinical Psychology
PhD (Psychology)
HPCSA No: PS0116807
Pr. nr: 0488127

POPIA MANUAL

Prepared in accordance with section 51 of the Protection of Personal Information Act of 2013.

DATE OF COMPILATION: 01/07/2023
DATE OF REVISION: 01/07/2023

 15 Kerkhof Street, George, 6529

 072 441 4143

 mariska@mariskacarter.co.za

 www.mariskacarter.co.za

CONSULTATION HOURS: Tuesdays (13h00 - 17h00), Wednesdays (13h00 - 17h00), Thursdays (08h00 - 12h00)





TABLE OF CONTENTS

- 1. Definition**
- 2. Introduction**
- 3. How the POPI manual works**
- 4. Head of practice contact details**
- 5. Practice information officer contact details**
- 6. Deputy information officer details**
- 7. Availability of this manual**
- 8. Lawful processing of personal information**
 - 8.1. Condition 1: Accountability**
 - 8.2. Condition 2: Processing Limitation**
 - 8.3. Condition 3: Purpose Specification**
 - 8.4. Condition 4: Further Processing Limitation**
 - 8.5. Condition 5: Information Quality**
 - 8.6. Condition 6: Openness**
 - 8.7. Condition 7: Security Safeguards**
 - 8.8. Condition 8: Data Subject Participation**
- 9. Policy Review**



1. DEFINITIONS

Biometrics:	A technique of personal identification that is based on physical, physiological, or behavioural characterisation, including blood typing, fingerprinting, DNA analysis, retinal scanning, and voice recognition
Child:	A natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning himself or herself
Competent person:	Any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child (i.e., the child's legal guardian)
Consent:	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.
De-identify:	In relation to personal information of a data subject, means to delete any information that: • identifies the data subject. • can be used or manipulated by a reasonably foreseeable method to identify the data subject. • can be linked by a reasonably foreseeable method to other information that identifies the data subject.
Direct marketing:	To approach a data subject, either in person, by mail or electronic communication, for the direct or indirect purpose of: • promoting, or offering to supply, in the ordinary course of business, any goods or services to the data subject. • requesting the data subject to make a donation of any kind and for any reason.
Electronic communication:	Any text, voice, sound, image or message, sent over an electronic communications network, which is stored in the network or in the recipient's terminal equipment, until it is collected by the recipient.
Head of a private body:	• in the case of a natural person, that natural person or any person duly authorised by that natural person • in the case of a partnership, any partner of the partnership or any person duly authorised by the partnership. • in the case of a juristic person: ○ the chief executive officer or equivalent officer of the juristic person, or any person duly authorised by that officer.



- the person who is acting as such or any person duly authorised by such acting person.

Information officer:	Head of a private body who ensures that the processing of personal information is done in a lawful manner, ensures compliance with POPI, deals with requests made to the private body in relation to POPI.
Manual:	POPIA Manual
Operator:	A person who processes personal information on behalf of the responsible party in terms of a contract or mandate, without coming under the direct authority of that party
PAIA:	Promotion of Access to Information Act (Act No.2 of 2000)
Person:	A natural person or a juristic person
Personal information:	Information about an identifiable, living, natural person, and, where it is applicable, an identifiable, existing juristic person, including, but not limited to: • information about the race, gender, sex, pregnancy, marital status, national, 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 • information relating to the educational, medical, financial, criminal or employment history of the person. • any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier, or other particular assignment to the person • the biometric information of the person • the personal opinions, views, or preferences of the person • 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. • the views or opinions of another individual about the person • the name of the person if it appears with other personal information about the person or if the disclosure of the name itself would reveal information about the person.
POPI Act:	Protection of Personal Information Act 4 of 2013
Practice:	The psychology practice of Dr Mariska Carter
Private body:	A natural person who carries or has carried on any trade, business, or profession but only in the capacity as a natural person; A partnership which carries or has carried on any trade, business, or profession; Any former or existing juristic person but excludes a public body.



- Processing:** Any operation or activity or any set of operations, whether or not by automatic means, pertaining to personal information, including the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation, or use; Dissemination by means of transmission, distribution, or making available in any other form; Merging, linking, restriction, degradation, erasure, or destruction of information
- Public body:** Any department of state or administration in the national or provincial sphere of government, or any municipality in the local sphere of government; Any other functionary or institution when: exercising a power or performing a duty in terms of the Constitution or a provincial constitution or exercising a public power or performing a public function in terms of any legislation.
- Public record:** A record that is accessible in the public domain and which is in the possession of, or under the control of, a public body, whether or not it was created by that public body.
- Record:** Any recorded information, regardless of form or medium, 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 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 (1) or more visual images are embodied to be capable, with or without the aid of some other equipment, of being reproduced.
- that's in the possession or under the control of a responsible party, whether or not it was created by a responsible party, regardless of when it came into existence.
- Regulator:** Information Regulator, established in terms of section 39 of the POPI Act
- Responsible party:** A public or private body, or any other person which, alone or together with others, determines why and how to process personal information
- Special personal information:** Personal information, as referred to in section 26 of the POPI Act:
- religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health, sex life or biometric information of a data subject



- criminal behaviour of a data subject, to the extent that the information relates to:
 - alleged commission by a data subject of any offence
 - proceedings about any offence allegedly committed by a data subject or the disposal of those proceedings.

2. INTRODUCTION

This manual is prescribed in terms of the Protection of Personal Information Act 4 of 2014 (the “POPI Act”), as amended or substituted from time to time. The POPI Act is intended to promote the right to privacy in the Constitution as well as protecting the flow of information and advancing the right of access to and protection of information.

The Practice is committed to effectively managing personal information in accordance with the POPI Act. The Practice is committed to protecting the privacy of its clients and employees and ensuring that their personal information is used appropriately, transparently, securely and in accordance with applicable laws.

The POPI Act applies to the processing of personal data, rather than a specific person or organisation. Therefore, whoever processes personal data must comply with the POPI Act and handle personal data according to POPIA’s data protection principles. Responsible parties determine the purpose for processing information, what information is processed, for how long and how it is processed. If an operator is involved, the responsible party will still determine the purpose for processing but will outsource the processing of the information to the operator. The Practice only uses operators that can meet the requirements of lawful personal information processing prescribed by the POPI Act and has a contractual agreement with each of its operators.

The Practice is a registered psychological services practice with the Board of Healthcare Funders (BHF) and with the Health Professions Council of South Africa (HPCSA). Through the provision of these services, the Practice is necessarily involved in collecting, using, and disclosing certain aspects of the personal information of its clients, employees (if applicable), and other stakeholders. As a responsible party, the Practice must comply with the POPI Act. The POPI Act requires the Practice to inform its clients and employees about the way their personal information is used, disclosed, and destroyed. This manual applies to the private psychology practice of Dr Mariska Carter (HPCSA number: PS116807; Practice number: 0488127) (“the Practice”). She is a registered clinical psychologist based in George, Western Cape. Dr Mariska Carter’s psychology practice provides psychotherapy services to adults and children. The Practice is in the health care sector and Dr Mariska Carter is a healthcare professional registered under the Health Professions Act of 1974 and is subject to the rules and regulations of the Health Professions Council of South Africa (HPCSA).



3. HOW THE POPI MANUAL WORKS

This Manual sets out the way the Practice deals with its clients' personal information and states the purpose for which the information is used and how it is used. This manual further outlines the business practices that will provide reasonable assurance that the rights of data subjects are protected and balanced with the legitimate business needs of the Practice.

4. HEAD OF PRACTICE CONTACT DETAILS

Name of Business/Practice: Dr Mariska Carter

Head of Practice: Dr Mariska Carter

Physical Address: 15 Kerkhof street, George central, George, Western Cape, 6529

Phone Number: 0724414143

E-mail Address: mariska@mariskacarter.co.za

Website: www.mariskacarter.co.za

5. PRACTICE INFORMATION OFFICER CONTACT DETAILS

Practice Information Officer: Dr Mariska Carter

Physical Address: 15 Kerkhof street, George central, George, Western Cape, 6529

Phone Number: 0724414143

Email Address: mariska@mariskacarter.co.za

6. DEPUTY INFORMATION OFFICER DETAILS

Name: N/A

Telephone Number: N/A

Fax Number: N/A

Email Address: N/A

7. AVAILABILITY OF THIS MANUAL

A copy of this manual is available for inspection, free of charge, at the offices of Dr Mariska Carter during her working hours or on the practice website at www.mariskacarter.co.za. It can be viewed on request from the Practice Information Officer. Any transmission costs or postage required in respect of hard copies of the Manual, will be for the account of the requester.

This manual will be updated from time to time as and when required.

The reference to legislation, subordinate legislation and supervision documents includes, amendments made from time to time (included but not limited to).

- Protection of Personal Information Act 4 of 2014 (the "POPI Act")
- Promotion of Access to Information Act 2 of 2000 (the "PAIA")
- Health Professions Act 56 of 1974



- National Health Act 61 of 2003
- Medical Schemes Act 121 of 1998
- Children's Act 38 of 2005
- Mental Healthcare Act 17 of 2002
- The Companies Act 71 of 2008
- Labour Relations Act 66 of 1995
- Basic Conditions of Employment Act 75 of 1997
- Employment Equity Act 55 of 1998
- Skills Development Levies Act 9 of 1999
- Unemployment Insurance Act 63 of 2001
- Electronic Communications and Transactions Act 25 of 2002
- Telecommunications Act 103 of 1996
- Electronic Communications Act 36 of 2005
- Consumer Protection Act 68 of 2008
- Broad-based Black Economic Empowerment Act 53 of 2003
- National Credit Act 34 of 2005
- Income Tax Act 58 of 1962
- Constitution of the Republic of South Africa, 1996 (the "Constitution").

8. LAWFUL PROCESSING OF PERSONAL INFORMATION

The Practice, as the responsible party, must adhere to the 8 conditions for the lawful processing of personal information:

- Condition 1: Accountability
- Condition 2: Processing limitation
- Condition 3: Purpose specification
- Condition 4: Further processing limitation
- Condition 5: Information quality
- Condition 6: Openness
- Condition 7: Security safeguards
- Condition 8: Data subject participation

8.1. CONDITION 1: ACCOUNTABILITY

Responsible party to ensure conditions for lawful processing.

The Practice is the responsible party that ensures it complies with the conditions and the measures that give effect to the conditions when it determines the purpose of processing, how it processes, and during the processing.

8.2. CONDITION 2: PROCESSING LIMITATION

Lawfulness of processing



The Practice must only process personal information lawfully and reasonably, in a way that does not infringe the privacy of the data subject.

Minimality

The Practice will only process personal information that is adequate, relevant, and not excessive, based on the purpose for processing that information. The Practice collects and processes data subjects' personal information in terms of several other laws associated with the functions performed by the Practice. As a health practitioner providing psychological services, the Practice may obtain personal information of potential and existing clients to determine the client's needs and objectives, among other regulatory and client personal requirements.

The Practice aims to have agreements in place with all third-party service providers to ensure a mutual understanding regarding the protection of clients' personal information. The Practice's product suppliers will be subject to the same regulations, as applicable to the Practice, in terms of the protection of clients' personal information. The practice will only provide the personal information needed for that third party to perform its obligations and services in terms of the contractual agreement between the practice and the said third party.

Consent, justification, and objection

The Practice will only process personal information if the:

- data subject, or a competent person (only where the data subject is a child), consents to the processing. For example, consent is obtained from clients before and/or during the assessment stage of the client relationship.
- processing is necessary to carry out actions for the conclusion, or performance, of a contract to which the data subject is party.
- processing complies with an obligation imposed by law on the responsible party.
- processing protects a legitimate interest of the data subject.
- processing is necessary for pursuing the legitimate interests of the Practice, or third parties/operators, to whom the information is supplied.

The Practice will have proof of the data subject's consent where consent is required. Where the data subject's consent for processing their personal information is required, the Practice will allow the data subject to withdraw their consent at any time as long as the lawfulness of the processing before the withdrawal of consent, or the processing where consent is not required, will not be affected by the withdrawal of consent.

A data subject can object to the processing of their personal information (by contacting the information officer and completing the prescribed Form 1, and on reasonable grounds relating to their situation), where the reason for the processing:

- protects a legitimate interest of the data subject.



- processing is necessary for the proper performance of a public law duty by a public body.
- processing is necessary for pursuing the legitimate interests of the responsible party.
- processing is necessary for pursuing the legitimate interests of a third party to whom the information is supplied,

the Practice must stop processing the data subject's related personal information, unless:

- legislation (including HPCSA guidelines) provides for the processing.
- processing is for purposes of direct marketing that is not by means of unsolicited electronic communications.

The applicable form – *Form 1 Objection to The Processing Of Personal Information In Terms Of Section 11(3) Of The Protection Of Personal Information Act, 2013 (Act No. 4 Of 2013)* – can be obtained at the offices of Dr Mariska Carter or on her website.

Collection directly from data subject

The Practice collects and processes the data subject's Personal Information to provide the client/data subject with access to its services and products, to help the Practice improve its offerings to the data subject, to support the contractual relationship between the Practice and data subject. The type and format of information the Practice collects will depend on the purpose for which it is collected and used.

The Practice will collect personal information directly from the data subject, except if:

- information is contained in or derived from a public record or has deliberately been made public by the data subject.
- data subject, or a competent person (only where the data subject is a child), consents to the collection of the information from another source (e.g., doctor, teacher)
- collection of the information from another source would not prejudice a legitimate interest of the data subject.
- collection of the information from another source is necessary:
 - to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences
 - to comply with an obligation imposed by law or to enforce legislation about the collection of revenue (in terms of the South African Revenue Service Act)
 - for the conduct of proceedings in any court or tribunal, which have commenced or are reasonably contemplated.
 - in the interests of national security
 - to maintain the legitimate interests of the responsible party
 - to maintain the legitimate interests of a third party to whom the information is supplied.
- compliance would prejudice a lawful purpose of the collection.



- compliance is not reasonably practicable in the circumstances of the case.

Retention of records

In accordance with Booklet 9 of the HPCSA, Guidelines on the Keeping of Patient Records, patient records are kept for a minimum period of six (6) years as from the date they become dormant, except where:

- “The patient is a minor, in which case records will be kept until the minor’s twenty- first birthday,
- The patient is mentally incompetent, in which case records are kept for the duration of the patient’s lifetime.” (Section 9.3)

Any other exceptions to the minimum period of 6 years laid out in Booklet 9, Section 9: Duration for the Retention of Health Records, including any future amendments made by the HPCSA to this document, will be adhered to.

Destruction of records

When a patient record has become obsolete (as set out by HPCSA guidelines), personal information captured in the file will be destroyed in a manner that still maintains the confidentiality of the information (e.g., shredding). Files will first be checked to confirm that they may be destroyed and also to ensure that there are no important original documents in the file, which would be returned to the holder. Electronic files will be permanently deleted from practice devices.

Rights of the Data Subject

The data protection laws give you certain rights in relation to the data we hold on you. These are:

- **the right to be notified.** This means that we must tell you how we use your Personal Information, and this is the purpose of this Privacy Policy.
- **the right of access.** You have the right to access the Personal Information that we hold on you. To do so, you should make a subject access request.
- **the right for any inaccuracies to be corrected.** If any Personal Information that we hold about you is incomplete or inaccurate, you can require us to correct it.
- **the right to have information deleted.** If you would like us to stop processing your Personal Information, you have the right to ask us to delete it from our systems where you believe there is no reason for us to continue processing it.
- **the right to restrict the processing** of the Personal Information. For example, if you believe the Personal Information, we hold is incorrect, we will stop processing it (whilst still holding it) until we have ensured that it is correct.
- **the right to portability.** You may transfer the Personal Information that we hold on you for your own purposes;
- **the right to object to the inclusion of any information.** You have the right to object to the way we use your Personal Information where we are using it for our legitimate interests.
- **the right to regulate any automated decision-making and profiling** of Personal Information. You have a right not to be subject to automated decision making in way that adversely affects your legal rights.



Where you have provided consent to our use of your Personal Information, you also have the unrestricted right to withdraw that consent at any time subject to contractual obligations. Withdrawing your consent means that we will stop processing the Personal Information that you had previously given us consent to use. There will be no consequences for withdrawing your consent; however, in some cases, we may continue to store and use the Personal Information where so permitted by having a legitimate reason for doing so or where required by law, regulation or by any other competent authorities. We may also not be able to continue our services to you.

You can read more about these rights within section 5 of POPIA.

8.3. CONDITION 3: PURPOSE SPECIFICATION

The very nature of the business conducted by the Practice requires the gathering of Personal information from a client and other relevant person/s (the latter being case dependent). Without such Personal information, the services requested from the Practice would not be possible.

The Practice will only collect information that it needs for a specific and lawful purpose, based on the relevant function or activity of the Practice or its operators. The Practice collects personal information and where applicable, special personal information from clients/data subjects for the purposes of billing, medical aid claims, contacting clients/data subjects for booking administration, assessment and treatment purposes, risk to self and others management, legal or contractual purposes, financial or tax purposes, treatment feedback and consent purposes. The Practice collects the following personal information for the purposes outlined above and for specific purposes described below:

Data Collected	Reason for Collection
Name and Surname	Identifying data for billing, claims submission and contact purposes
ID number, Date of birth and age	Identifying data for billing, claims submission and assessment and treatment purposes
Copy of ID book	Confirmation of identity
Copy of medical aid card	Confirmation of medical aid details
Marital Status:	Assessment purposes
Residential Address	Billing and debt collection purposes
Cell phone number and E-mail address	Contact purposes
Occupation and Employment Information	Assessment and Treatment purposes
Employer/School	Billing, debt collection and contact purposes
Medical Aid Provider, Plan, Number, Main Member, Dependents (with corresponding date of births)	Billing and claims purposes
Emergency contact details	Contact purposes and personal risk management
Source of referral (if applicable)	Referral and treatment information



School and Grade	Contact purposes, assessment, and treatment purposes
Medical Information	Assessment and treatment purposes
Educational Information	Assessment and treatment purposes
Language	Communication purposes
Legal activities	Referral purposes, Assessment, and treatment purposes
In the Case of Minors, additional information include:	
Copy of child's birth certificate / ID book	Confirmation of identity
Mother's/Legal guardian's name and contact details; Copy of ID book	Confirmation of identity, Contact, consent, billing, claim, risk management and feedback purposes
Father's/Legal guardian's name and contact details; Copy of ID book	Confirmation of identity, Contact, consent, billing, and claim purposes

The personal information is provided on a voluntary basis. However, withholding information will likely have a negative impact on the therapeutic process, in that the provision of psychotherapy services will not be possible.

Complaint

If you have a concern about any aspect of the practice's privacy practices, you can make a complaint. This will be acted upon promptly. To make a complaint, please contact the practice via one of the methods set above. You undertake to first make a good faith attempt to resolve same with the Practice. If you are not first satisfied with the practice's response to your complaint, you have the right to then lodge a complaint with our supervisory authority, the Information Regulator. You can find details about how to do this on their website: <https://www.justice.gov.za/infoereg/>.

8.4. CONDITION 4: FURTHER PROCESSING LIMITATION

The Practice may share personal information of data subjects/clients with the following third parties, to the extent that is needed for the third parties to perform their duties or contractual obligations:

- Billing company
- Accounting company
- Medical Aids
- Debt collection agencies (when necessary)
- Hospitals (when necessary)
- Other health care practitioners for the purposes of referral, treatment, assessment, and/or supervision.
- Any third parties as required or allowed for by law.
- Third parties, as requested, consented to, or agreed to in a contract by the data subject.

8.5. CONDITION 5: INFORMATION QUALITY



The Practice, as the responsible party, will take reasonable steps to ensure that the personal information is complete, accurate, not misleading and updated, where necessary, based on the purpose for which the personal information is collected or further processed. The practice informs all clients in its informed consent forms, to assist the Practice in keeping the information accurate and up to date by notifying the practice of any changes that it needs to be aware of.

8.6. CONDITION 6: OPENNESS

Documentation

The Practice will maintain the documents of all processing operations that it is responsible for, and which information must be included in the POPI and/or PAIA Manual, relating to the:

- purpose of the processing
- description of the categories of data subjects and of the information or categories of information relating thereto
- recipients, or categories of recipients, to whom the personal information may be supplied.
- planned transborder flows of personal information.
- general description, allowing a preliminary assessment of the suitability of the information security measures to be implemented by the Practice, to ensure the confidentiality, integrity and availability of the information that is to be processed.

The Practice will update its POPI and/or PAIA Manual, to include the required information for protecting personal information and publish the updated POPI and PAIA Manual, as required. All POPI related documentation, including this manual, is stored in a POPI file which is locked away in a safe cupboard within the practice. All electronic POPI related documentation will be stored in a password protected file on the practice's computer. The POPI and PAIA manuals, as well as application/request forms, are available at the practice and on the practice's website.

Notification to data subject when collecting personal information.

The Practice will ensure that the data subject is aware of the:

- information that is collected
- source from which the information is collected, where the information is not collected directly from the data subject.
- name and address of the Practice, as the responsible party
- purpose for collecting the information.
- fact that the information they supply is either voluntary or mandatory.
- consequences of failing to provide the information.
- law authorising or requiring the collecting of the information.



- fact that, where applicable, the Practice intends to transfer the information to a third country or international organisation, and the level of protection afforded to the information by that third country or international organisation.
- other relevant information which is necessary in the specific circumstances in which the information is, or is not, to be processed to enable processing for the data subject to be reasonable, such as:
 - recipient, or category of recipients, of the information
 - nature or category of the information
 - existence of the right of access to and the right to rectify the information collected.
 - existence of the right to object to the processing of personal information
 - right to lodge a complaint to the Information Regulator and the contact details of the Information Regulator

The Practice collects and further processes information of clients, as data subjects, for functions or activities, including, but not limited to:

- Performing the initial assessments as well as ongoing assessments
- Providing the products or services, or related products or services, to clients, and/or carrying out services reasonably related thereto.
- Confirming, verifying, and updating information
- Conducting market or client satisfaction research
- Audit and record keeping
- Legal or similar proceedings
- Activities relating to maintaining and improving the client relationship.
- Providing communication about the Practice, Therapists, its products, services and regulatory matters which may affect clients.
- Sharing information with other relevant health practitioners, educators, product suppliers and service suppliers with whom we have relationships, to process information on our behalf, or to those who provide services to the practice and/or the client.
- Complying with legal and regulatory requirements or when it is otherwise allowed by law.

8.7. CONDITION 7: SECURITY SAFEGUARDS

Confidentiality of personal information

By virtue of the provisions of Section 32(1)(a) of POPIA, most, if not all, Personal information gathered from and regarding clients will be exempt from the general POPIA provisions prohibiting the collection and processing of such Personal information. It is, however, a policy of the Practice to obtain the consent of all relevant parties before gathering and/or processing Personal information.



All Client related Personal information is subject to an obligation of confidentiality by virtue of the profession under which the Practice falls, as well as South African legislation. As such, all Personal information provided will be treated as strictly confidential, with the following exceptions:

- with a client's (or that client's guardian in applicable cases) express consent.
- where Personal information is required by the client's medical aid or other person responsible for payment of the Practice's professional fees (where applicable) to process claims for treatment provided by the Practice or for the Practice's administration.
- where the Practice is obliged by law to divulge information.
- where consultation with other mental health professionals is viewed as being necessary.
- where the client poses a danger to him- or her- self, or another person.
- where the client's referral source or family doctor require feedback regarding his or her treatment. In such a case, information will only be supplied once discussed with the client or guardian (where applicable).
- in the case of a deceased Client, with the written consent of the next of kin or the executor of the deceased's estate.

About the treatment of minors: doctors, teachers, and other people (depending on the client) may need to be consulted to gain additional information. Furthermore, such people may be better able to support and help the client if the Practice is allowed to communicate essential information or management strategies to them. Should the Head of Practice believe that Personal information regarding the client should be shared with any of the aforesaid categories of persons care and discretion will be used, and the guardian and client will first be consulted, and their permission obtained.

Security measures of personal information

The Practice, as the responsible party, or acting as the operator, **MUST** secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable, technical, and organisational measures to prevent:

- loss of, damage to, or unauthorised destruction of personal information
- unlawful access to or processing of personal information by taking reasonable measures to:
- identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control.
- establish and maintain appropriate safeguards against the risks identified.
- regularly verify that the safeguards are effectively implemented.
- ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.



The Practice has taken to following measures to protect personal information:

Protection of hardcopy data:

- Paper-based records are kept in a locked cupboard within the practice.

Protection of electronic data:

- The internet is an open medium and it cannot be guaranteed that any information you send to the practice by email or other electronic means will not be intercepted or tampered with; any transmission is at your own risk. Once the practice has received your information, it will use appropriate procedures and security features to prevent unauthorised access.
- Electronic records containing identifying and/or personal patient information are password protected and stored on password protected electronic devices.
- The software on the practice's computer is regularly updated and has virus protection software.
- All operators have signed an agreement with the Practice that they also need to adhere to POPIA, including taking reasonable steps to store and protect personal information of data subjects.
- **Emails:** The practice e-mail account is password protected and can only be accessed through the practice's computer which is also password protected. Reports containing personal/confidential information are password protected in that the receiver of the document will need a password to open the attached report. Emails also have a disclaimer.
- **Telephone:** Any messages and/or voicemails left by potential or existing clients are made to the practice's mobile phone, which is password protected.

Protection of information by third parties:

- Third party service providers who have access to personal information are required to sign an agreement to protect the personal information of the clients or patients at this practice.
- Medical aids with whom personal information is shared will be assumed to be responsible for protection of that personal information in accordance with their own POPI compliance procedures based on the Protection of Personal Information Act 4 of 2013.

Planned Trans-Border Flow of Personal Information

The Practice does not have any planned trans-border flow of personal information.

Links to external websites

The practice website or social media pages may, from time to time, contain links to and from other websites. If you follow a link to any of these websites, please note that these websites have their own privacy policies and that the practice does not accept any responsibility or liability for these policies or how such websites collect and use your data. Please check these policies before you submit any Personal Information to these websites.



Security compromises

If there is a breach of personal information, the Regulator, and the data subject will be informed as soon as is reasonably possible after the discovery of the compromise, considering the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the Practice's information system. The Practice, as the responsible party, may only delay notifying the data subject if a public body responsible for the prevention, detection or investigation of offences, or the Regulator, determines that notification will impede a criminal investigation by the public body or the Regulator.

The contractual agreements between the practice and operators also stipulate that operators need to inform the Practice of any suspected security breaches.

The Practice will notify the data subject about a personal information compromise in at least one (1) of the following ways:

- sent by e-mail to the data subject's last known e-mail address.
- placed in a prominent position on the website or social media platform of the responsible party.

8.8. CONDITION 8: DATA SUBJECT PARTICIPATION

Access to personal information

A data subject that provides the Practice with adequate proof of identity may ask the Practice, as the responsible party to confirm whether the Practice holds personal information about the data subject, as well as for a copy of the record of personal information about the data subject held by the Practice. Please note that any such access request to records may be subject to a payment of a legally allowable fee, as stipulated in the Practice's PAIA Policy. Persons requesting access to data are directed to the PAIA Manual and Form C for procedures involving application to access information.

The Practice may or must refuse to disclose information or records requested by the data subject to which the grounds for refusal of access to records are set out in the applicable sections of the PAIA (Refer to the Practice's PAIA manual for details).

Correction of personal information

The Practice would appreciate it if the data subject would take the necessary steps to keep his/her Personal Information accurate and up to date by notifying the Practice of any changes it needs to be aware of.

After taking reasonable steps to confirm the data subject's identity, a data subject may request the Practice, by completing Form 2, as the responsible party, to:

- Correct, update, or delete personal information about the data subject in its possession or under its control which is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or obtained unlawfully.



- destroy, or delete, a record of personal information about the data subject, which the Practice, as the responsible party, is no longer authorised to retain because it is no longer necessary for achieving the purpose for which the information was collected or subsequently processed.

Where the Practice, as the responsible party, receives a request to correct or delete, personal information, it will, as soon as reasonably practicable:

- correct or update the information.
- destroy or delete the information.
- notify a data subject who has made a request to correct or delete their personal information, of the action taken due to the request.
- provide the data subject, to their reasonable satisfaction, with credible evidence, in support of the information having been corrected or deleted.
- where agreement cannot be reached between the Practice and the data subject and if the data subject requests, take reasonable steps in the circumstances to attach to the information, in a way that it will always be read with the information, an indication that a correction of the information has been requested, but has not been made.

Where the Practice, as the responsible party, has taken steps that result in a change to the data subject's personal information and the changed information has an impact on decisions that have been, or will be, taken in respect of the data subject in question, it **MUST**, if reasonably practicable, inform each person, body or responsible party to whom the personal information has been disclosed, of those steps. If the Practice refuses to correct, update, destroy, or delete information, it will inform the data subject of this refusal and provide the reasons thereof. The practice will always function within all the relevant legal and ethical codes to reach its outcome. The applicable form – *Form 2 Request For Correction Or Deletion Of Personal Information Or Destroying Or Deletion Of Record Of Personal Information In Terms Of Section 24(1) Of The Protection Of Personal Information Act, 2013 (Act No. 4 Of 2013)* – can be obtained at the offices of Dr Mariska Carter or on her website.

Manner of access

- The procedures to follow regarding requests to access personal information/records are outlined in detail in the **PAIA manual**.
- Requests for correcting, updating, or deleting personal information/records can be made to the Practice Information Officer, whose details are supplied in the POPI and PAIA manuals.

Processing of personal information of children

The Practice, as the responsible party, MAY process personal information of children IF it is:

- carried out with the prior consent of the legal guardian (competent person)



- necessary for the establishment, exercise, or defence of a right or obligation in law
 - necessary to comply with an obligation of international public law.
 - for historical, statistical or research purposes, to the extent that:
 - the purpose serves a public interest, and the processing is necessary for the purpose concerned; or,
 - it appears to be impossible or would involve a disproportionate effort to ask for consent,
- and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the child to a disproportionate extent.
- personal information has deliberately been made public by the child with the consent of a competent person.

Disclosure of personal information

All information provided will be treated as strictly confidential but may be disclosed in the circumstances outlined in Condition 7 (Confidentiality of Personal information).

Third party service providers who have access to personal information are asked to sign an agreement to protect the personal information of the clients/patients at the Practice. Medical Aids with whom Personal information is shared will be assumed to be responsible for protection of that personal information in accordance with their own POPI compliance procedures based on the Protection of Personal Information Act 4 of 2013. Any client/patient information that is shared with other healthcare practitioners for the purposes of supervision or research will be de-identified.



9. POLICY REVIEW

The policy will be reviewed annually, updated, if necessary, and the latest version will be adopted and approved by the Practice as represented by the information officer.

Policy approval and information

Policy owner	Mariska Carter
Policy type	Compliance
Approver's signature	
Approved by (this version)	Mariska Carter
Approval date (this version)	18/07/2023
Version number	V01

<u>Summary of policy history</u>				
<u>Version number</u>	<u>Drafted/adapted/reviewed by</u>	<u>Creation/review date</u>	<u>Approved by</u>	<u>Approval date</u>
V01	Mariska Carter	18/07/2023	Mariska Carter	18/07/2023