Personal Information Management Policy

of

Samantha Jane Leeferink Physiotherapy

Initial approval date	01/06/2021
Revision number	1
Date of last review	01/06/2021
Date of next review	01/06/2022

TABLE OF CONTENTS

1. PURPOSE OF POLICY

The purpose of this Policy is to outline what the persons, to whom this Policy applies, may or may not do in the execution of their duties to ensure the protection of the personal information of patients, and other persons and entities (collectively referred to as "data subjects") in the possession or under the control of Samantha Jane Leeferink Physiotherapy("the Practice"). The Policy is intended to protect the Practice from exposure to legal liability.

2. EXPLANATION OF TERMS

2.1 **"Child"** refers to *"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 him- or herself."*

2.2 **"Competent person"** refers to a person who may legally consent on behalf of a patient.

2.3 **"Data subject"** refers to the person to whom the personal information relates. Data subjects in the practice setting include patients, their next-of-kin or persons who may act on their behalf, practitioners, employees, referring doctors and any other person or entity of which the Practice has personal information in its possession or under its control.

2.4 **"De-identify**", in relation to personal information of a data subject, means to delete any information that—

2.4.1 identifies the data subject;

2.4.2 can be used or manipulated by a reasonably foreseeable method to identify the data subject; or

2.4.3 can be linked by a reasonably foreseeable method to other information that identifies the data subject,

and **"de-identified"** has a corresponding meaning.

2.5 **"HPCSA"** refers to the Health Professions Council of South Africa.

2.6 **"PAIA"** means the Promotion of Access to Information Act 2 of 2000 and the Regulations made in terms thereof.

2.7 **"PAIA Manual"** means the manual compiled by the Practice as required in terms of section 51 of PAIA read with section 17 of POPIA.

2.8 **"Personal Information"** refers to information relating to identifiable, living, natural persons as well as identifiable, existing juristic persons, and includes, but is not limited to -

2.8.1 information relating to 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;

2.8.2 information relating to the education or the medical, financial, criminal or employment history of the person;

2.8.3 any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

2.8.4 the biometric information of the person;

2.8.5 the personal opinions, views or preferences of the person;

2.8.6 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;

2.8.7 the views or opinions of another individual about the person; and

2.8.8 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.

The personal information of living natural persons (i.e. human beings) and existing juristic persons (e.g. companies) is protected under POPIA.

2.9 **"POPIA"** means the Protection of Personal Information Act 4 of 2013 and the Regulations made in terms thereof.

2.10 **"Processing"** means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including -

2.10.1 the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

2.10.2 dissemination by means of transmission, distribution or making available in any other form; or

2.10.3 merging, linking, as well as restriction, degradation, erasure or destruction of information.

For purposes of this Policy, 'processing' includes any activity that can be undertaken in respect of personal information.

2.11 **"Public record"** means 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.

2.12 **"Record"** means any recorded information—

2.12.1 regardless of form or medium, including any of the following—

2.12.1.1 writing on any material;

2.12.1.2 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;

2.12.1.3 label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;

2.12.1.4 book, map, plan, graph or drawing;

2.12.1.5 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;

2.12.2 in the possession or under the control of a responsible party;

2.12.3 whether or not it was created by a responsible party; and

2.12.4 regardless of when it came into existence.

2.13 **"Re-identify**", in relation to personal information of a data subject, means to resurrect any information that has been de-identified, that—

2.13.1 identifies the data subject;

2.13.2 can be used or manipulated by a reasonably foreseeable method to identify the data subject; or

2.13.3 can be linked by a reasonably foreseeable method to other information that identifies the data subject,

and **"re-identified"** has a corresponding meaning.

2.14 **"Special personal information"** refers to information, which relates to a data subject's religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, criminal behaviour or biometric information.

2.15 **"SOP"** refers to a Standard Operating Procedure of the Practice.

2.16 **"Unique identifier"** refers to any identifier that is assigned to a data subject and is used by a responsible party (e.g. the Practice) for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

3. APPLICATION

This Policy applies to the Practice, its directors / partners, employees (including temporary and part-time employees), contractors and locums (collectively referred to as "practitioners and employees"), who have access to or process personal information. This includes any activity or operation, whether automated or not, concerning personal information, such as collect, use, disseminate, store or disclose that information, for and on behalf of the Practice.

4. LEGAL FRAMEWORK

4.1 The following laws and their Regulations govern, amongst others, the processing and confidentiality of personal information and must be considered in conjunction with this Policy:

- 4.1.1 Constitution of the Republic of South Africa ("RSA") (Act 108 of 1996);
- 4.1.2 Electronic Communications and Transactions Act 25 of 2002;
- 4.1.3 Health Professions Act 56 of 1974;
- 4.1.4 National Health Act 61 of 2003;
- 4.1.5 PAIA; and
- 4.1.6 POPIA.

4.2 The Ethical Rules and other relevant policies and directives of the HPCSA must also be considered especially the HPCSA's *Guidelines for Good Practice in the Healthcare Professions* in respect of

- 4.2.1 *Confidentiality: Protecting and Providing Information* (Booklet 5);
- 4.2.2 *Seeking Patients' Informed Consent: The Ethical Considerations* (Booklet 4);

4.2.3 *Guidelines on the Keeping of Patient Records* (Booklet 9); and

4.2.4 *Ethical Guidelines on Social Media* (Booklet 16).

4.3 If any conflict occurs between a provision of this Policy and the law, the law prevails.

5. OTHER POLICIES

This Policy must be considered in conjunction with other policies and SOPs related to the processing of personal information, such as the Privacy Statement, Record-Keeping Policy, Information Technology (IT) Policy and the Website Terms and Conditions of the Practice.

6. INFORMATION OFFICER

The Information Officer of the Practice is:

Name: Samantha Jane Leeferink

Position: Owner

Contact telephone number: 0842700833

E-mail address: samantha@sjlphysio.co.za

If any uncertainty exists about the application of this Policy or if there is any query or question in relation to the processing of personal information in the performance of duties or the discharge of functions, the Information Officer must be contacted for support and guidance.

7. PERSONAL INFORMATION

7.1 For purposes of this Policy, 'personal information' includes all personal information of any data subject in the possession or under the control of the Practice, including personal information of deceased persons, but not information of juristic persons that no longer exist.

7.2 Personal information must be handled with utmost care to secure and maintain the confidentiality and integrity of that information as required in terms of the law.

7.3 Practitioners registered at the HPCSA are under a statutory obligation to maintain confidentiality of patient information.

7.4 An obligation of confidentiality must be imposed on employees and practitioners. This will occur through their employment or other agreements or amendments to these agreements.

8. INFORMATION NOT SUBJECT TO THIS POLICY

Information, from which the identity of data subjects cannot be determined, such as trend analyses and aggregate reporting, is not subject to this Policy. In legal terms this refers to de-identified information that cannot be re-identified.

9. DATA SUBJECTS' RIGHTS

9.1 Data subjects have the following rights:

9.1.1 to have their personal information processed in accordance with the conditions for the lawful processing of personal information as set out in POPIA;

9.1.2 to be notified that their personal information is being collected;

9.1.3 to be notified that their personal information has been accessed or acquired by an unauthorised person;

9.1.4 to establish whether the Practice holds personal information about them and to request access to that information;

9.1.5 to request, where necessary, the correction, destruction or deletion of their personal information;

9.1.6 to object, on reasonable grounds to the processing of their personal information as provided for in POPIA;

9.1.7 to object to the processing of their personal information for purposes of direct marketing;

9.1.8 not to have their personal information processed for purposes of direct marketing by means of unsolicited electronic communications, except as provided for in POPIA;

9.1.9 not to be subject to a decision, which is based solely on the automated processing of their personal information and which provides profiles of them, except as provided for in POPIA; and

9.1.10 to submit a complaint to the Information Regulator or institute civil proceedings regarding the alleged interference with the protection of their personal information.

10. COLLECTION OF PERSONAL INFORMATION

10.1 Personal information may only be collected, if it is required by the Practice for lawful purposes related to its function and activities and as provided for in relevant legislation. No more

information than what is necessary must be collected.

10.2 The purposes for which personal information is collected by the Practice must, amongst others, be communicated to the affected data subjects, as may be necessary from time to time. Refer also to paragraph 16 below. The Practice uses a Privacy Statement and Privacy Poster, amongst others, to communicate the prescribed information to patients and other data subjects.

10.3 Personal information must as far as possible be collected directly from the patient or other person to whom it relates. It may be collected from other sources (e.g. the next-of-kin of a patient or the patient's medical scheme), in the following circumstances:

10.3.1 if the person to whom the information relates (i.e. the patient or other data subject) has provided written consent;

10.3.2 the information is contained in a public record;

10.3.3 the information has deliberately been made public by the data subject (e.g. on social media);

10.3.4 it will not prejudice a legitimate interest of the data subject (e.g. collection of information from patients' next-of-kin may fall in this category or from the patient's medical scheme to determine benefits available for treatment);

10.3.5 to comply with an obligation imposed by law (e.g. the Medical Schemes Act and the Consumer Protection Act contain requirements for information that must occur on invoices);

10.3.6 it is necessary to maintain the legitimate interests of the Practice or of a third party to whom the information is supplied;

10.3.7 obtaining the information from the data subject is not reasonably practicable in the circumstances (e.g. the patient is sedated in hospital);

10.3.8 obtaining the information from the data subject will prejudice a lawful purpose of the collection; or

10.3.9 it is necessary for proceedings in a court or tribunal.

What constitutes a 'legitimate interest' as contemplated in paragraphs 10.3.4 and 10.3.6 must be determined with reference to the facts of the situation. The Information Officer must be requested for guidance in this regard.

11. ACCESS TO AND USE OF PERSONAL INFORMATION

11.1 Practitioners and employees may only have access to personal information if it is reasonably

required for the performance of their duties and functions. For example, only employees that require access to patients' health information for the performance of their functions, should have access to this information. Practitioners and employees must not attempt to gain access beyond their access privileges and may not bypass security controls without the approval of the Information Officer.

11.2 Access to the accounting records or other commercially sensitive information of the Practice is subject to approval by the Head of the Practice and the Information Officer.

11.3 Third parties (such as service providers and professional advisers) may only be provided with access to personal information if it is reasonably required for the performance of their functions with approval from the Head of the Practice and the Information Officer subject to a written agreement or confidentiality undertaking, as may be appropriate in the circumstances. Their use of the information must be monitored by the Information Officer or another designated person.

11.4 Personal information may only be used for lawful purposes related to the business of the Practice as permitted in terms of the law or otherwise with the written consent of the patient or other data subject. Personal information to which a practitioner or an employee gained access as part of discharging his/her functions at the Practice may not be used by the practitioner or employee for any other purpose than that for which the information was provided or obtained.

11.5 Legal basis for processing of personal information

11.5.1 *Personal information, other than special personal information*, may be processed (e.g. used, stored and disseminated) in the following circumstances:

11.5.1.1 with consent of the data subject;

11.5.1.2 for the conclusion or performance of a contract to which the data subject is party, for example, when a patient is accepted at the practice for the performance of medical services (a patient stands in a contractual relationship with the Practice);

11.5.1.3 for compliance with an obligation imposed by law (e.g. compiling an invoice for a patient);

11.5.1.4 for the protection of a legitimate interest of the data subject unless the data subject objects on reasonable grounds on the form prescribed by POPIA; or

11.5.1.5 for the pursuit of the legitimate interests of the Practice or of a third party to whom the information is supplied unless the data subject objects on reasonable grounds on the form prescribed by POPIA.

What constitutes a 'legitimate interest' as contemplated in paragraphs 11.5.1.4 and 11.5.1.5 must be determined with reference to the facts of the situation. The Information Officer must be requested for guidance in this regard.

11.5.2 Special care must be taken when *personal information of children* and other sensitive information of persons, i.e. *special personal information*, is processed. Special personal information is information relating, amongst others, to a data subject's race or ethnic origin, health or criminal behaviour as well as biometric information. Special personal information and personal information of children may, in general, be processed in the following circumstances:

11.5.3 with the consent of the data subject or a competent person (e.g. a parent or legal guardian in respect of a child);

11.5.4 for the establishment, exercise or defence of a right or an obligation in law;

11.5.5 for historical, statistical or research purposes provided that—

11.5.5.1 the purpose serves a public interest and the processing is necessary for that purpose; or

11.5.5.2 it is impossible or would involve a disproportionate effort to obtain consent,

and sufficient guarantees are provided to ensure that the processing does not adversely affect the privacy of the data subject to a disproportionate extent;

11.5.6 the information has deliberately been made public by the data subject and in the case of a child with the consent of a competent person.

11.5.7 Practitioners may process any type of *special personal information* if it is necessary for the proper treatment and care of the patient.

11.5.8 *Health information* of a patient may be processed for the proper treatment and care of the patient and for administrative purposes. **Invoices may only be submitted directly to medical schemes with the written consent of the patient or a person who may act on behalf of the patient**.

11.5.9 The Practice may process *health information* of employees for the implementation of the provisions of laws or collective agreements, which create rights dependent on the health of the employee, or for the reintegration of or support to an employee entitled to benefit in connection with sickness or work incapacity (e.g. sick leave).

11.5.10 *Race-related information* may be processed with consent of the patient unless it is required for the proper treatment and care of the patient. The Practice may process race-related information of employees to comply with obligations imposed by law, such

as the Employment Equity Act 55 of 1998. The processing of race-related information of other data subjects require their written consent unless it is permitted by law.

11.5.11 The Practice processes the types of *personal information* of its data subjects in accordance with the legal bases as set out in the table below.

PERSONAL INFORMATION PROCESSED	LEGAL BASIS / JUSTIFICATION
Patients (Adult)	
Name and surname, contact details, gender, identity number / date of birth, funder, next-of-kin, photos, videos	Agreement; historical, statistical and research purposes; National Health Act; Medical Schemes Act; Health Professions Act, Consumer Protection Act; consent
Health information	Treatment and care; administration of practice; historical, statistical and research purposes; National Health Act; Medical Schemes Act, POPIA, Health Professions Act
Race	Treatment and care
Patients (Children)	
Name and surname, contact details, gender, identity number / date of birth, funder, next-of-kin, photos, videos	National Health Act; common law; historical, statistical and research purposes; Medical Schemes Act, Health Professions Act; Consumer Protection Act; consent of competent adult; perform agreement with competent adult
Health information	Treatment and care; administration of practice; historical, statistical and research purposes; National Health Act; Medical Schemes Act, POPIA, Health Professions Act

Race	Treatment and care
Practitioners and Staff	
Name and surname, contact details, gender, identity number / date of birth, qualifications, registration, employment-related information, bank details, photos	Employment contract, Basic Conditions of Employment Act, Labour Relations Act, Employment Equity Act, Health Professions Act; information made deliberately public; public records
Race	Employment Equity Act
Health information	Occupational Health and Safety Act, Basic Conditions of Employment Act, POPIA
Referring and Other Health Care Practitioners	
Name and surname, contact details	Health Professions Act; POPIA
Referral letter	Health Professions Act; POPIA
Service Providers, Vendors and Suppliers	
Name and surname, contact details, VAT number, bank details, BEE status	Agreement; Information made deliberately public; POPIA
Other Public and Private Bodies	
Names, contact details, official information	Public records; Information made deliberately public; POPIA
Next-of-kin (Patients and Staff)	
Names and contact details	Legitimate interest of patient and practice; administration of practice; POPIA

11.6 There could be circumstances when personal information may only be lawfully used for certain restricted purposes, which are defined in legislation. This will, for example, occur when the accuracy of the information in the possession or under the control of the Practice is contested by a data subject. Refer further in this regard to paragraph 22.

11.7 Practitioners and employees, who have resigned, terminated their contracts with the Practice, or have been dismissed, must be assessed as to their continuing need for access to personal

information in the possession or under the control of the Practice. Access to such information may only continue with permission of the Head of the Practice and the Information Officer.

11.8 Practitioners and employees who are subject to disciplinary action or who face criminal charges, may only have access to personal information with the express permission of the Head of the Practice and the Information Officer.

12. PRE-AUTHORISATION BY THE INFORMATION REGULATOR

12.1 The Information Officer must obtain pre-authorisation from the Information Regulator for the following processing activities of the Practice as prescribed in POPIA:

12.1.1 processing of _____ (unique identifiers e.g. file numbers) of _____ (data subjects), which identifiers are linked to information processed by _____ (responsible party);

12.1.2 credit reporting; and

12.1.3 transferring of _____ (special personal information) and the personal information of children to _____ (third party) in _____ (countries).

12.2 Processing of the abovementioned information must be suspended if required by the Information Regulator or comply with conditions imposed by the Regulator, if applicable.

13. CONSENT

13.1 Where processing of personal information occurs on the basis of consent, such consent must be voluntary, specific, informed and unambiguous. Refer to paragraph 25 for consent requirements related to unsolicited electronic marketing.

13.2 Consent must be in writing. Consent may also be obtained through the use of data messages as determined by the Head of the Practice / Information Officer.

13.3 In the case of patients, the relevant patient should provide the consent. Children who are able to independently consent to treatment must consent to the processing (including the disclosure) of their personal information. The age of 12 can be used as a guideline to determine whether the child must independently consent to the processing of his/her personal information, provided that such a child is able to independently consent to medical treatment. Depending on the mental capacity and maturity of the child the age could be higher or lower

than 12 years. This must be determined at the point of care by the relevant practitioner.

13.4 Where a patient cannot independently consent, a person authorised in terms of the law may provide the necessary consent.

13.5 Consent may be withdrawn at any time. Such withdrawal must be respected by practitioners and employees. All processing activities conducted before withdrawal of the consent remain valid and lawful. Any processing activities conducted after withdrawal of the consent must be authorised in terms of the law.

13.6 The Information Officer must in conjunction with the IT support function at the Practice design a mechanism to record consent and the withdrawal of consent by data subjects, which information must be available to practitioners and authorised employees.

14. FURTHER PROCESSING

14.1 If the Practice has collected personal information for a specific purpose (e.g. to treat a patient) and would like to process it further (e.g. for research purposes, for collection of an outstanding amount, etc.) such further processing must be compatible with the purpose for which the information was originally collected.

14.2 Further processing of personal information in the Practice may occur in the following circumstances:

14.2.1 with written consent of the data subject or a competent person in the case of a child;

14.2.2 the information is available in or collected from a public record;

14.2.3 the information has deliberately been made public by the data subject;

14.2.4 it is necessary for proceedings in a court or tribunal;

14.2.5 it is necessary to prevent or mitigate a serious and imminent threat to public health or safety or to the life or health of the data subject or another individual (e.g. exposure to COVID-19); or

14.2.6 the information is only used for historical, statistical or research purposes and will not be published in an identifiable form.

14.3 The Information Officer must determine which other forms of further processing of information is acceptable with reference to the following criteria:

14.3.1 the relationship between the purpose of the further processing and the purpose for which the information has been collected;

14.3.2 the nature of the information;

14.3.3 the consequences of such further processing for the data subject;

14.3.4 the manner in which the information has been collected; and

14.3.5 any contractual rights and obligations between the parties.

15. SHARING AND DISCLOSURE OF PERSONAL INFORMATION

15.1 Personal information may only be shared with or disclosed to other practitioners or employees to fulfil the purposes identified at the time of the collection of that information, or for a purpose reasonably related to those purposes (e.g. sharing with the accountant for billing purposes), provided that these practitioners or employees require the information reasonably and lawfully for the performance of their duties or functions.

15.2 Other disclosures of personal information require the written consent of the data subject unless such disclosures are permitted in terms of the law (e.g. reporting of notifiable conditions under the National Health Act or in the circumstances permitted in terms of PAIA).

15.3 Special care must be taken when personal information of children and other special personal information of data subjects are shared or disclosed to ensure that the privacy of the relevant data subject is not compromised.

15.4 Legislation and the consent provided by the patient must be considered to determine which disclosures of his/her information are permitted before disclosing any personal information of that patient to a third party.

15.5 An SOP must be prepared by the Information Officer indicating when personal information of patients may be lawfully disclosed to third parties.

15.6 Invoices containing ICD-10 codes may only be submitted to funders with the patients' written consent.

15.7 No personal information of any data subject may be shared on social media without the express permission of the Information Officer.

15.8 Any disclosure of personal information of any data subject must be recorded in the Practice in the place and manner as determined by the Information Officer and must include the nature of the information disclosed and the recipient's identity.

16. NOTIFICATIONS TO DATA SUBJECTS

16.1 When the Practice collects personal information, it must communicate certain information to the relevant data subjects. This will assist to make the processing of that information reasonable.

16.2 The following information must be communicated:

16.2.1 the information being collected;

16.2.2 the source of collection, if not collected from the data subject;

16.2.3 the name and address of the Practice;

16.2.4 the purpose for which the information is collected;

16.2.5 whether the supply of the information by the data subject is voluntary or mandatory;

16.2.6 the consequences, if the information is not provided;

16.2.7 any law requiring or authorising the collection;

16.2.8 whether the Practice intends to transfer the information to another country and the level of protection afforded to the information by that country;

16.2.9 the recipient or category of recipients of the information;

16.2.10 the nature of the information;

16.2.11 the data subject has a right to access and request rectification of the information;

16.2.12 the right of the data subject to object to the processing of the information as contemplated in POPIA; and

16.2.13 the right of the data subject to lodge a complaint with the Information Regulator and the Regulator's contact details.

16.3 The above information must only be communicated once to the data subject provided that any subsequent information collected is of the same kind and the purpose of collection remains the same.

16.4 The above information listed must as far as possible be communicated to the data subject before collection of the information.

16.5 The above information does not have to be communicated in the following circumstances:

16.5.1 consent by the data subject or competent person;

16.5.2 there will not be prejudice to a legitimate interest of the data subject;

16.5.3 collection of the information is necessary to comply with an obligation imposed by law;

16.5.4 collection of the information is necessary for proceedings in a court or tribunal;

16.5.5 communication of the information will prejudice a lawful purpose of the collection;

16.5.6 communication of the information is not reasonably practicable in the circumstances;

16.5.7 the information will not be used in a form that will identify the data subject; or

16.5.8 the information will be used for historical, statistical or research purposes.

16.6 The Practice uses various mechanisms to communicate the specified information. The information is communicated to patients through the Practice's Privacy Statement and Privacy Poster. The Information Officer must ensure that the information is communicated to other data subjects in a suitable manner.

17. SECURING PERSONAL INFORMATION

17.1 The Practice is committed to ensure the confidentiality and integrity of the personal information in its possession or under its control in order to protect such information from unauthorised access, collection, use, disclosure, dissemination, copying, modification, storage or disposal.

17.2 The Practice's IT Policy / SOP governs the use of and access to information through the Practice's IT infrastructure, portable computers, smart phones and other handheld devices and includes directives related to the downloading of programmes, applications and information from the Internet, anti-virus software, as well as good practice related to suspicious e-mails and related matters. This Policy / SOP is integral to and must be read with this Policy.

17.3 The Information Officer must on a regular basis conduct a risk assessment in respect of the personal information in the possession or under the control of the Practice as contemplated in the law and implement the necessary safeguards.

17.4 The following security measures must be followed to ensure that the personal information is appropriately protected:

17.4.1 Each interface that gives a practitioner or an employee access to personal information contained in any record in the possession or under the control of the Practice, including print-outs of electronic records, must be considered confidential and reasonable steps must be taken to protect these records from unauthorised access.

17.4.2 Hard copy records and printouts of electronic records containing personal information must not be left unattended on desks, printers or photocopiers or similar equipment, or in offices during practitioners' or employees' absence from their work areas or offices, even for brief periods, or in areas (e.g. reception) where unauthorised persons may access them. They must be securely stored in a lockable drawer, cabinet or safe with the keys removed.

17.4.3 Matters involving personal information should never be discussed in public areas. Telephone discussions, interviews and consultations, which involve the disclosure of

personal information about a person, must be conducted in areas and circumstances where confidentiality can be maintained. Special care must be taken in reception areas to ensure that personal information of patients is treated with the necessary care and that confidentiality is ensured.

17.4.4 Individual offices must be locked outside of business hours.

17.4.5 Practitioners and employees must only use secure routes to send personal information and always mark the information as confidential. The risks and consequences of unauthorised or accidental release of personal information must be assessed when transmitting information by e-mail or any other means.

17.4.6 Practitioners and employees must only obtain and keep the minimum amount of personal information necessary to perform their duties or functions.

17.4.7 Practitioners and employees must only copy and/or share records containing personal information with other persons when it is necessary to perform their duties or functions, and sharing of personal information may only occur with authorised persons as set out in this Policy, a relevant SOP or in accordance with the law.

17.4.8 If practicable, documents must be converted into an electronic format and be stored on an encrypted device.

17.4.9 Record storage areas must be locked when not in use.

17.4.10 Access to server rooms and storage areas for electronic records must be managed with key card access.

17.4.11 Documents, including printouts of records, containing personal information may only be destroyed through the secure mechanisms provided by the Practice (such as secure shredding services) and in accordance with the relevant SOP. These documents may not be disposed of at home, while travelling or by placing them in a dustbin.

17.5 Removing hard copy documents from the Practice:

17.5.1 Practitioners and employees may not remove hard copy documents containing personal information from the Practice without the permission and knowledge of the Information Officer.

17.5.2 The Information Officer must monitor and log their removal and return, including the following, in a written record:

17.5.2.1 the type and format of the documents;

17.5.2.2 the personal information included in those documents;

17.5.2.3 the purpose for which the documents are being removed;

17.5.2.4 the time period for which the documents are expected to be out of the office; and

17.5.2.5 when the documents have been returned.

17.5.3 Only the documents necessary to perform a duty or function must be removed.

17.5.4 The Information Officer must report any missing documents to the Head of the Practice within 24 hours of becoming aware thereof. This requirement is essential for the Practice to investigate any potential loss of personal information.

17.5.5 Any authorised person, who removes documents containing personal information from the Practice, must take reasonable and practicable steps to protect the documents from unauthorised disclosure or damage. For example, the documents must not be left unattended, including in bags at airports, in locked but empty cars or in any other unattended location, but must where possible, be kept in the personal possession of the authorised person.

17.6 The Practice must continually review and update its security policies and controls as technology changes to ensure ongoing personal information security.

18. PROCESSING OF INFORMATION BY THIRD PARTIES

If any person or entity processes personal information of any data subject on behalf of the Practice, written agreements must be entered into with the relevant person or entity, which contains, amongst others, the information prescribed in POPIA and ensures that the Practice is protected against any claim, which may arise if a security breach occurs.

19. RETENTION AND STORAGE OF RECORDS

The Practice must retain and store records containing personal information as provided for in the law. For this purpose, the Practice has prepared a Record-keeping Policy, which stipulates the time periods for which documents must be retained, and how the information must be stored. Personal information may only be deleted from records and records containing personal information may only be destroyed in accordance with this Policy.

20. ACCESS TO RECORDS BY DATA SUBJECTS

20.1 A data subject has a right of access to his/her/its personal information in the possession or

under the control of the Practice subject to the provisions of PAIA, which allows the Practice to refuse access to records or information in certain circumstances, for example, when it relates to an unreasonable disclosure of information of a person.

20.2 The Practice has prepared a PAIA Manual to facilitate access to the information in its possession and under its control. The PAIA Manual contains information about the records and personal information in the possession or under the control of the Practice, the procedure for persons to request access to any of these records or information and the applicable fees.

20.3 The PAIA Manual will be updated regularly.

20.4 The PAIA Manual is available at reception, on the Practice's website and from the Information Officer.

20.5 The following persons may provide records of their personal information to patients: _____. Care must be taken that third parties' information is not included in those records that are being shared unless that information may be shared lawfully.

20.6 If access to information is granted to a data subject, he/she/it must be advised of his/her/its right to request a correction of that information as provided in POPIA.

21. ENSURING ACCURACY OF PERSONAL INFORMATION

21.1 When personal information is collected, used or stored, reasonable efforts must be made to ensure that the information is accurate and complete, especially where the information may be used to make a decision about a person, such as a patient.

21.2 Persons in respect of whom the Practice has personal information in its possession or under its control may request corrections to their information in order to ensure accuracy and completeness on the prescribed form.

21.3 Authorised employees may update or correct the contact details, addresses and medical scheme details of patients and those of persons who may act on their behalf, when necessary. Other corrections of personal information and requests to delete information must be requested in writing by the patients and other data subjects from the Information Officer on the prescribed form, providing sufficient detail to identify the relevant personal information and the correction or deletion required.

21.4 If any personal information is inaccurate or incomplete, the Information Officer must ensure that the information is corrected as required by legislation (i.e. POPIA read with the National Health Act and the Guidelines on the Keeping of Patient Records of the HPCSA). The Information

Officer must ensure that the corrected information is provided to all persons and entities to whom the information has been previously disclosed (e.g. funders), if the amended information will affect any decision made on the basis of that information.

21.5 When the accuracy of the personal information in the possession or under the control of the Practice is contested, the Practice may only process this information as set out in paragraph 22 during the period in which the accuracy of the information is verified.

21.6 If a requested correction to or deletion of information is not made, the correction/deletion request must be noted at the relevant information together with the reason for not doing it as required in terms of POPIA, if requested by the data subject.

21.7 An audit trail must be logged of all corrections made to electronic records or attempts to alter electronic records and their metadata.

22. RESTRICTION OF PROCESSING

22.1 The processing of personal information by the Practice must be restricted in the following circumstances:

22.1.1 accuracy of the information is contested by the data subject;

22.1.2 the information is no longer needed by the Practice, but is maintained for proof;

22.1.3 processing is unlawful and the data subject requests restriction of use instead of destruction or deletion of that information; or

22.1.4 the data subject requests that the information must be transmitted into another automated processing system.

22.2 In the above circumstances, the information must be clearly identified as “restricted use” by the Information Officer in conjunction with the IT support function, and until the restriction is lifted, the Practice may only -

22.2.1 store the information;

22.2.2 use the information for purposes of proof;

22.2.3 process the information with consent of the data subject:

22.2.4 process the information for the protection of the rights of another person; or

22.2.5 process the information in the public interest.

22.3 The Practice must inform the data subject before the restriction is lifted.

23. SENDING INFORMATION ACROSS THE BORDERS OF THE RSA

23.1 Personal information of data subjects may only be sent to third parties outside of the RSA, if it is necessary and with the approval of the Information Officer who must consider whether any of the following circumstances is present before approval is given:

23.1.1 the third party is subject to a law, binding corporate rules (as prescribed in POPIA) or a binding agreement, which provides an adequate level of protection of that information and which is similar to the protection under POPIA; or

23.1.2 with consent of the data subject; or

23.1.3 it is necessary in terms of a contract between the data subject and the Practice; or

23.1.4 it is necessary for a contract concluded between the Practice and the third party in the interest of the data subject; or

23.1.5 the transfer is for the benefit of the data subject, it is not reasonably practicable to obtain his/her/its consent and if it was possible the data subject was likely to provide consent; and

23.1.6 where personal information is not adequately protected in another country as required by POPIA, special personal information and personal information of children may only be sent to a third party in that country after pre-authorisation has been obtained from the Information Regulator as required by POPIA (refer to paragraph 12).

23.2 'Cloud' storage of records must comply with the requirements of POPIA.

24. HISTORICAL, STATISTICAL AND RESEARCH PURPOSES

24.1 Personal information may, in certain circumstances, be used for historical, statistical and research purposes provided that it is not published in an identifiable form. The Information Officer must be consulted and approve all processing of personal information for historical, statistical and research purposes to ensure that it may occur and that safeguards are in place to protect the privacy of data subjects.

24.2 Special personal information and personal information of children may only be processed for historical, statistical or research purposes if

24.2.1 the purpose serves a public interest and the processing is necessary for the purpose; or

24.2.2 it is impossible or would involve a disproportionate effort to obtain consent; and

24.2.3 there are sufficient guarantees in place to ensure that the privacy of the data subject is not adversely affected to a disproportionate extent.

25. MARKETING ACTIVITIES

25.1 Direct marketing, including unsolicited electronic marketing, of products and services of the Practice may only be directed to patients and other persons who have provided consent for such purposes as prescribed.

25.2 Direct marketing must be distinguished from communication with patients regarding their treatment and care or other practice-related matters (e.g. appointment reminders), as may be required from time to time.

25.3 A data subject may object to the processing of his/her/its personal information for purposes of direct marketing.

25.4 The Practice may process personal information for purposes of unsolicited electronic marketing of bona fide patients in the following circumstances:

25.4.1 their contact details were obtained when they became patients of the Practice;

25.4.2 for the purpose of the direct marketing of the Practice's own services; and

25.4.3 if they were given a reasonable opportunity to object to the use of their electronic details when the information was collected and every time a marketing communication is sent to them (i.e. "opt out").

25.5 The Practice must obtain consent from persons who have not provided consent as contemplated in paragraph 25.4 in the prescribed form before any marketing activities are directed to them.

25.6 Direct marketing communications must contain the Practice's details, including contact details to which the recipient may send a request that such communications cease.

25.7 All direct marketing initiatives must comply with the provisions of the Consumer Protection Act, for example, with reference to the days on and times at which such communications may be sent, and any rule or directive of the HPCSA.

26. PROFILING

26.1 Decisions, which are based solely on the automated profiles of persons, for example, related to their performance at work or health, and which may have legal consequences or have a substantial impact on those persons, are not permitted unless it is done in terms of an

agreement with the person that meets the requirements of POPIA.

26.2 Profiling of any person or entity may only occur after consultation with and approval by the Head of the Practice and the Information Officer.

27. INFORMATION REGULATOR

27.1 The Practice is accountable to the Information Regulator to ensure that personal information is processed lawfully and without transgressing the privacy of any data subject.

27.2 If the law does not authorise the processing of personal information, which is required by the Practice, and if the Practice cannot obtain consent for such processing, the Information Officer must approach the Information Regulator for permission or an exemption from POPIA.

27.3 All decisions of the Information Regulator impacting on the processing of personal information by the Practice must be communicated to practitioners and employees and this Policy and/or other policies must be updated, as may be necessary, to reflect these decisions.

28. SECURITY COMPROMISES

28.1 Any compromise of the security of personal information in the possession or under the control of the Practice, which includes unauthorised and unlawful access to such information, poses serious risks to the Practice. Significant fines may, for example, be imposed by the Information Regulator and/or damages may be awarded by the courts against the Practice.

28.2 If there are reasonable grounds to believe that the personal information of a person has been accessed or acquired by an unauthorised person, it must be reported without delay to the Information Officer, who in turn must advise the Head of the Practice. Where the Information Officer is involved or allegedly involved in a security compromise, such compromise or alleged compromise must be report to the Head of the Practice / the auditor of the Practice / accountant of the Practice.

28.3 All security or alleged security compromises will result in an investigation of the incident.

28.4 A practitioner or an employee, who is responsible for a security compromise, intentionally or unintentionally, in respect of personal information as well as a person who fails to report a security compromise or potential security compromise of which he/she is aware must receive appropriate remedial advice and training and may be subject to appropriate action such as disciplinary action in the case of employees.

28.5 Access to personal information by practitioners and employees who deliberately or repeatedly violate security mechanisms or compromise the privacy of a data subject's personal information must be suspended until the appropriate remedial action has been determined.

28.6 The Information Officer is responsible to report security compromises to the Information Regulator and the persons whose privacy has been compromised as provided for in POPIA.

29. COMPLAINTS

29.1 Any complaint, concern or question regarding the processing of personal information by the Practice must be addressed to the Information Officer. If the Information Officer is involved or allegedly involved in the matter, the complaint, concern or question must be addressed to the Head of the Practice / auditor of the Practice / accountant of the Practice.

29.2 Practitioners and employees, who are concerned or dissatisfied with the processing of their personal information by the Practice, may lodge a grievance as provided for in the Practice's workplace policies.

29.3 The Information Officer must make serious efforts to resolve queries and complaints pertaining to the processing of personal information.

29.4 Any person, who is concerned or dissatisfied with the processing of his/her/its personal information by the Practice, may lodge a complaint with the Information Regulator and he/she/it may not be prohibited from doing so.

30. VERIFICATION OF COMPLIANCE WITH POLICY AND AUDIT

30.1 The Practice reserves the right to audit all processing activities of personal information in its possession or under its control from time to time to ensure compliance with this Policy and the law.

30.2 The Information Officer may verify compliance with this Policy and the law through various methods, including but not limited to periodic walk-throughs, business tool reports, compliance audits (internal and external) and any form of electronic monitoring.

31. NON-COMPLIANCE WITH THIS POLICY

31.1 Any non-compliance or alleged non-compliance with this Policy or any relevant legislation will result in an investigation of the non-compliance or alleged non-compliance.

31.2 Any violation of this Policy or any relevant legislation will be dealt with in terms of applicable employee policies or another appropriate mechanism, as may be available and applicable.

32. IMPLEMENTATION OF THIS POLICY

32.1 The Information Officer must ensure that all practitioners and employees are provided with a copy of or access to this Policy and are trained in every aspect of this Policy.

32.2 All practitioners and employees must agree in writing to comply with this Policy, such other additional documents arising from this Policy as may be approved from time to time and all relevant legislation before being given access or further access to any personal information.

33. EFFECTIVE DATE OF POLICY

This Policy comes into operation on the date of approval by the Head of the Practice and supersedes all other policies and related documents on the subject matter from the effective date.

34. POLICY REVISION

This Policy must be reviewed and updated at least on an annual basis.

Signature of the Head of the Practice

Signature of the Information Officer

Date of Approval: 01/06/2021