KEIMED ANAESTHESIOLOGY

PROTECTION OF PERSONAL INFORMATION & PROMOTION OF ACCESS TO INFORMATION POLICY

INTRODUCTION

The Practice is obliged to comply with the Protection of Personal Information Act 4 of 2013 (POPI) as well as the Promotion of Access to Information Act 2 of 2000 (PAIA), given that it processes the personal information of its employees, service providers, clients and other data subjects from time to time as well as that there may be requesters of information relating to the Practice and its operations.

The Practice guarantees its commitment to protecting data subject privacy as well as ensuring that their personal information is used appropriately, transparently, securely and in accordance with applicable laws. This is in line with the Constitutional provisions.

POPI requires the Practice to inform its data subjects as to how their personal information is collected, processed, secured, disclosed and destroyed. This Policy sets out the manner in which the Practice deals with such personal information as well as stipulates the general purpose for which such information is used. It also addresses the standards expected of employees of the Practice in respect of their conduct in this regard.

The Information Officer shall ensure that a PAIA guide is posted on the website in English (as provided by the Information Regulator) and that the said Guide is available at each of its offices for public inspection. The list of records that are voluntarily disclosable and/ or available without a requester having to request access thereto shall be kept and updated monthly and/ or whenever the contents change. The said list shall be posted on the website, registered with the Information Regulator and kept in hard copy at the offices of the Practice. A requester who requests access to a record under PAIA statute shall complete the necessary form and follow the protocols required.

Appropriate stakeholders should be made aware of the contents of this Policy when their consent is requested for the processing of their personal information or when there are interactions with data subjects.

The provisions of this policy must be read along with the relevant practices and procedures that are used to operationalise the purpose hereof.

COLLECTION OF PERSONAL INFORMATION

The Practice collects stores and processes personal information pertaining to data subjects including its employees, service providers, clients and other stakeholders. The type of information collected and processed will depend on the purpose for which it is collected and will be processed for that scope of application only. Whenever appropriate, the Practice will inform the data subject of the information required, the purpose thereof, the rights of participation and the other relevant provisions contained at law.

The Practice must indicate to the data subject the consequence of failing to provide such personal information. For example, the Practice may not be able to employ an individual without certain personal information relating to that individual or the Practice may not be in a position to render services to a client in the absence of certain information which is required.

Examples of the personal information the Practice collects includes, but is not limited to information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person –

a) 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;

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

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

d) the biometric information of the person;

e) the personal opinions, views or preferences of the person;

f) 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;

g) the views or opinions of another individual about the person; and

h) 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.

COLLECTION OF EMPLOYEE INFORMATION

For the purposes of this Policy, “employees” include potential, past and existing employees of the Practice.

The Practice will, when appointing new employees, require information, including, but not limited to that listed above, from the prospective employee in order to process the employee’s information on the Practice’s system. Such information is reasonably necessary for the Practice’s record purposes as well as to ascertain if the prospective employee meets the requirements for the position to which he or she is being appointed and is suitable for such appointment.

The Practice will use and process such employee information, as set out below, for purposes including, but not limited to, its employment records and to make lawful decisions in respect of that employee and its business.

USE OF EMPLOYEE INFORMATION

Employees’ personal information will only be used for the purpose for which it was collected and intended. This would include, but is not limited to:

a) submissions to the Department of Employment and Labour

b) submissions to the Receiver of Revenue

c) for audit and recordkeeping purposes

d) in connection with legal proceedings

e) in connection with and to comply with legal and regulatory requirements

f) in connection with any administrative functions of the Practice

g) disciplinary action or any other action to address the employee's conduct or capacity

h) in respect of any employment benefits that the employee is entitled to

i) pre-and post-employment checks and screening

j) any other relevant purpose to which the employee has been notified of

k) any compliance requirements at law.

Should information be processed for any other reason that is not in the legitimate interests of the employee, the Practice will inform the employee accordingly.

The Practice acknowledges that personal information may only be processed if certain conditions are met which, depending on the merits include -

a) The employee consents to the processing

b) The processing is necessary to attend to justifiable rights and obligations, for example contractual fulfilment

c) The processing complies with an obligation imposed by law on the Practice

d) Processing protects a legitimate interest of the employee

e) Processing is necessary for pursuing the legitimate interests of the Practice or of a third party to whom information is supplied.

COLLECTION OF CLIENTS AND/ OR SERVICE PROVIDER INFORMATION

For purposes of this Policy, clients include potential, past and existing clients.

The Practice collects and processes its clients' personal information, such as that mentioned hereunder. The type of information will depend on the need for which it is collected and will be processed for that purpose only. Further examples of personal information collected from clients include, but is not limited to:

a) To practice staff and third parties for the purposes of treating and managing me in terms of a doctor-and-patient relationship;

b) Disclosing my medical diagnoses and procedure to the relevant Medical Scheme in order to verify services rendered;

c) Communicating with other persons in as much as it relates to my treatment and management;

d) Communicating with third parties who have undertaken to indemnify me for the costs of my treatment and management, or part thereof, including Medical Schemes and the administrators, where relevant;

e) My medical records may also be provided to an authorised third-party in the event of a valid audit of clinical practice;

f) Anaesthetists may need to obtain relevant medical information relating to me from other health-care providers (e.g. pathologists or radiologists) for my optimal care or for the legal submission of an account for the purposes of collecting monies outstanding from me;

g) I agree to this disclosure;

h) The client's identity number, name, surname, address, postal code;

i) The client's residential and postal address;

j) Contact information;

k) Banking details;

l) Practice registration number;

m) Full name of the legal entity;

n) Tax and/or VAT number;

o) Details of the person responsible for the client's account;

USE OF CLIENT AND SERVICE PROVIDER INFORMATION:

The client's personal information will only be used for the purpose for which it was collected and as agreed, if any such agreement is required at law. This may include, but not be limited to:

a) Providing products and/ or services to clients

b) In connection with sending accounts and communication in respect of services rendered

c) Referral to other service providers

d) Confirming, verifying and updating client details

e) For audit and record keeping purposes

f) In connection with legal proceedings

g) In connection with and to comply with legal and regulatory requirements or when it is otherwise allowed by law.

The Practice acknowledges that personal information may only be processed if any of the conditions set out hereunder are met:

a) Client consents to the processing

b) The processing is necessary to attend to rights and obligations that are justifiable, including fulfilling contractual provisions

c) The processing complies with an obligation imposed by law on the Practice

d) Processing protects a legitimate interest of the party

e) Processing is necessary for pursuing the legitimate interests of the Practice or of a third party to whom information is supplied.

DISCLOSURE OF PERSONAL INFORMATION

Subject to legislative provisions providing the contrary, the Practice may share data subject's personal information with third parties as well as obtain information from such third parties for reasons set out above.

The Practice may also disclose data subject's information where there is a duty or a right to disclose in terms of applicable legislation, a contractual obligation, the law or where it may be necessary to protect the Practice's rights.

SAFEGUARDING PERSONAL INFORMATION AND CONSENT

It is a requirement of POPI to adequately protect the personal information the Practice holds and to avoid unauthorised access and use of personal information.

The Practice shall review its technical and operational security controls and processes on a regular basis to ensure that personal information is secure.

The Practice shall appoint an Information Officer who is responsible for the encouragement of compliance with the conditions of the lawful processing of personal information and other provisions of POPI and PAIA.

INFORMATION OFFICER DETAILS:

FULL NAME:	Jonathon Garth Dowie
DESIGNATION:	Associate
EMAIL:	enquiries@keimed.co.za
CONTACT NUMBERS:	043 701 8300
FAX NUMBER:	043 701 8304
POSTAL ADDRESS:	P O Box 15292
	Beacon Bay
	5205
PHYSICAL ADDRESS:	Life Beacon Bay Hospital, Level 1
	32 Quenera Drive
	Beacon Bay
	5241

Each new employee will be required to sign an employment contract containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPI.

Every employee currently employed within the Practice will be required to sign an addendum to their employment contract containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPI.

The Practice's Service Providers who fall within the definition of "operators" will be required to enter into a written agreement guaranteeing their commitment to the Protection of Personal Information.

Consent to process client information is obtained from data subjects (or a person who has been given authorisation from the client to provide the client's personal information) during the introductory, appointment and needs analysis stage of the relationship.

SECURITY BREACHES

Should the Practice detect a security breach on any of its systems that contain personal information, the Practice shall take the required steps to assess the nature and extent of the breach in order to ascertain if any information has been compromised.

The Practice shall activate its Incident Response Plan which includes the notification of the affected parties and the Information Regulator should it have reason to believe that personal information has been compromised. Such notification shall only be made where the Practice can identify the data subject to which the information relates. Where it is not possible it may be necessary to consider website publication and whatever else the Information Regulator prescribes.

Notification will be provided in writing by means of either:

- email
- registered mail
- place on our website.

The notification shall provide the following information where possible:

a) description of possible consequences of the breach,

b) measures taken to address the breach,

c) recommendations to be taken by the data subject to mitigate adverse effects,

d) the identity of the party responsible for the breach.

In addition to the above, the Practice shall notify the Regulator of any breach and/or compromise to personal information in its possession and work closely with and comply with any recommendations issued by the Regulator.

The following provisions will apply in this regard –

a) The Information Officer will be responsible for overseeing the investigation;

b) The Information Officer will be responsible for reporting to the Information Regulator within 2 working days of a breach / compromise to personal information;

c) The Information Officer will be responsible for reporting to the Data Subject(s) within 2 working days of a breach/ compromise to personal information;

d) The timeframes above are guidelines and depending on the merits of the situation may require earlier or later reporting.

ACCESS AND CORRECTION OF PERSONAL INFORMATION

Data subjects have the right to request access to any personal information that the Practice holds about them.

Data subjects have the right to request the Practice to update, correct or delete their personal information on reasonable grounds. Such requests must be made to the Practice's Information Officer (see details above) or submitted via the website "Information Officer Portal".

Where an employee or client objects to the processing of their personal information, the Practice may no longer process said personal information. The consequences of the failure to give consent to process the personal information must be set out before the employee or client confirms his/her objection.

The data subject must provide reasons for the objection to the processing of his/her personal information.

RETENTION OF RECORDS

The Practice shall ensure the safeguarding and protection of all personal information or data. The Practice is obligated to retain certain information as prescribed by law. This includes but is not limited to the following:

With regard to the Companies Act, No. 71 of 2008 and the Companies Amendment Act No 3 of 2011, hard copies of the documents mentioned below must be retained for 7 years:

- Any documents, accounts, books, writing, records or other information that a Practice is required to keep in terms of the Act
- Notice and minutes of all shareholders meetings, including resolutions adopted and documents made available to holders of securities
- Copies of reports presented at the annual general meeting of the Practice
- Copies of annual financial statements required by the Act and copies of accounting records as required by the Act.

The Basic Conditions of Employment No. 75 of 1997, as amended requires the Practice to retain records relating to its staff for a period of no less than 3 years.

AMENDMENTS TO THIS POLICY

Amendments to this Policy will take place from time to time subject to the discretion of the Practice and pursuant to any changes in the law. Such changes will be brought to the attention of employee's clients where it affects them.

STANDARDS OF CONDUCT REQUIRED OF EMPLOYEES

These are contained in the provisions within this POPI policy, the employment contract, the disciplinary code, the electronic communications and social media policy as well as any other document relating to employees, the following standards of conduct and practice and their accompanying underlying principles must be complied with at all times and a breach thereof may result in serious disciplinary action and even dismissal for a first offence.

PHYSICAL RECORDS AND ASSETS

All physical records containing personal information (PI) as well as any hardware, devices or similar equipment must always be protected from unauthorised access and / or damage and / or loss and / or other prejudice.

SYSTEMS AND PLATFORMS

Compliance with security requirements in respect of, for example, the following areas is crucial:

a) Changing, storage and sharing of usernames and passwords

b) Data back-ups and protection

c) Limitations on the use of personal devices such as external hard drives or similar storage options, mobile phones and the like.

INTERNAL AND EXTERNAL POSTING OF PERSONAL INFORMATION OF PRACTICE DATA SUBJECTS

A prohibition on the sharing and/ or posting of PI on any platforms outside of those that are Practice approved under specific conditions as well as a total ban on posting and / or transmitting PI outside of the Practice on social media and / or any other similar platform.

CONDITIONS TO BE OBSERVED WHEN COLLECTING OR PROCESSING PI

The following principles must be complied with when dealing with PI and if there is any doubt, the written authority of the Information Officer must be obtained by the employee prior to the said processing –

ACCOUNTABILITY

The employee must ensure that the conditions and all the measures that give effect to such conditions are complied with at the time of the determination of the purpose and means of the processing and during the processing itself.

PROCESSING LIMITATION

Personal information must be processed

a) lawfully; and

b) in a reasonable manner that does not infringe the privacy of the data subject.

This includes considerations of minimality and adequacy given the purpose for which it is intended. In addition -

a) The data subject or a competent person (data subject is a child) consents to the processing; and / or

b) The purpose is to carry out actions for the conclusion or performance of a contract; and / or

c) Processing complies with an obligation imposed by law on the responsible party; and / or

d) Processing protects a legitimate interest of the data subject; and / or

e) Processing is necessary for the proper performance of a public law duty by a public body; and / or

f) Processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied; and / or

g) Collection must be directly from the data subject, except as otherwise provided for unless the information is contained in or derived from a public record or has deliberately been made public by the data subject.

PURPOSE SPECIFICATION

PI is collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party.

FURTHER PROCESSING LIMITATION

Further processing of personal information must be compatible with the purpose for which it was collected and consider -

a) the consequences of the intended further processing for the data subject

b) the manner in which the information has been collected; and

c) any contractual rights and obligations between the parties.

SECURITY SAFEGUARDS

Employees must secure the integrity and confidentiality of personal information in their possession or under their control by taking appropriate, reasonable technical and organisational measures to prevent—

a) loss of, damage to or unauthorised destruction of personal information; and

b) unlawful access to or processing of personal information.

Employees must take reasonable measures to—

c) identify all reasonably foreseeable internal and external risks to personal information in its possession or under their control;

d) establish and maintain appropriate safeguards against the risks identified;

e) regularly verify that the safeguards are effectively implemented; and

f) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

Employees must have due regard to generally accepted information security practices and procedures which may apply to the situation generally or be required in terms of specific industry or professional rules and regulations.

Additional security safeguards guidelines to be observed –

- Only share PI on a need-to-know basis,
- Security systems including anti-virus and malware detections (and install updates immediately)
- Secure and back-up files
- Encryption
- Password security, protection and authentication
- Use multifactor identification,
- BYOD protocols agreed before allowing use
- Keep mobile devices safe
- Accessing suspect links, pop-ups and unknown mails prohibited

- Only use secure Wi-Fi
- Firewall protection at work and at home
- Report any security concerns and warnings
- Limit employee and user access in general
- Monitor 3rd parties
- Provide education and training
- Be cautious with unvetted USB’s
- Install security software updates
- Be aware of social engineering.

Implementation Date: 1 July 2021

Authorized by: Jonathon Dowie (Information Officer for KeiMed Anaesthesiology)

This document and its procedures may be amended from time to time at the discretion of management subject to prevailing laws and best practice.

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)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018

[Regulation 2.]

Note:

1. *Affidavits or other documentary evidence as applicable in support of the objection may be attached.*
2. *If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.*
3. *Complete as is applicable.*

A	**DETAILS OF DATA SUBJECT**
Name(s) and surname/ registered name of data subject:	
Unique Identifier/ Identity Number	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number / E-mail address:	
B	**DETAILS OF RESPONSIBLE PARTY**
Name(s) and surname/ Registered name of responsible party:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number/ E-mail address:	
C	**REASONS FOR OBJECTION IN TERMS OF SECTION 11 (1) (*d*) to (*f*) (***Please provide detailed reasons for the objection*****)**

Signed at on this day of 2 .

Signature of data subject/designated person

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)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018

[Regulation 3.]

☐ **Correction or deletion** of the personal information about the data subject which is in possession or under the control of the responsible party.

☐ **Destroying or deletion** of a record of personal information about the data subject which is in possession or under the control of the responsible party **and who is no longer authorised to retain the record of information**

A	**DETAILS OF THE DATA SUBJECT**
Name(s) and surname/ registered name of data subject:	
Unique identifier/ Identity Number:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number/E-mail address:	
B	**DETAILS OF RESPONSIBLE PARTY**
Name(s) and surname / registered name of responsible party:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number/ E-mail address:	
C	**INFORMATION TO BE CORRECTED/DELETED/ DESTRUCTED/ DESTROYED**
D	**REASONS FOR *CORRECTION OR DELETION OF THE PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24 (1) (*a*) WHICH IS IN POSSESSION OR UNDER THE**

	CONTROL OF THE RESPONSIBLE PARTY; and or REASONS FOR *DESTRUCTION OR DELETION OF A RECORD OF PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24 (1) (*b*) WHICH THE RESPONSIBLE PARTY IS NO LONGER AUTHORISED TO RETAIN (*Please provide detailed reasons for the request*)

Signed at on this day of 2 .

Signature of data subject/designated person