NETMED
FAMILY PRACTITIONERS

PROTECTION OF PERSONAL INFORMATION (POPI) POLICY

TABLE OF CONTENTS

1. BACKGROUND

Netmed Strand is a registered company ("the Company"), Practice Registration number 1481878 who provides professional medical services to the public.

The right to privacy is an integral human right, recognised and protected by the South African Constitution and in the Protection of Personal Information Act, Act No 4 of 2013 ("POPIA"). The POPI Act aims to promote the protection of privacy through providing guiding principles that are intended to be applied to the processing of personal information in a context-sensitive manner.

Through the provision of our service delivery in the medical care industry, the Company is involved in the collection, use and disclosure of certain aspects of the personal information of employees, clients, service providers, and other stakeholders.

A person's right to privacy entails having control over his or her personal information and being able to conduct his or her affairs relatively free from unwanted intrusions. Given the importance of privacy, the Company is obligated to comply with the POPI Act and is committed to protecting its clients' privacy and ensuring that their personal information is utilised appropriately, transparently, securely and in accordance with applicable laws.

2. PURPOSE

This policy demonstrates the Company's commitment to protecting the privacy rights of data subjects, as well as protecting the Company from risks associated with the protection of personal information, in the following manner:

2.1 Through stating desired behaviour and directing compliance with the provisions of the POPI Act and best practice.

2.2 By cultivating a company culture that recognises privacy as a valuable human right.

2.3 By developing and implementing internal controls for the purpose of managing the compliance risk associated with the protection of personal information.

2.4 By creating business practices that will provide reasonable assurance that the rights of data subjects are protected and balanced with the legitimate business needs of the Company.

2.5 By assigning specific duties and responsibilities to control owners, including the appointment of an Information Officer in order to protect the interests of the Company and data subjects.

2.6 By raising awareness through training and providing guidance to individuals who process personal information so that they can act confidently and consistently.

3. DEFINITIONS

"Biometrics" means a technique of personal identification that is based on physical, psychological, or behavioural characterisation including blood typing, fingerprinting, DNA Analysis, retinal scanning and voice recognition;

"Board" means the Board of Netmed Strand;

"Directors" means the Directors of Netmed Strand;

"Consent" means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information;

"Data subject" means the person to whom the personal information relates;

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

(a) Identifies the data subject;
(b) Can be used or manipulated by a reasonably foreseeable method to identify the data subject; or

(c) Can be linked by a reasonably foreseeable method to other information that identifies the data subject,

And **"de-identified"** has a corresponding meaning;

"Electronic communication" means any text, voice, sound or image 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;

"Employees" means all key individuals, representatives and staff employed by Netmed Strand,

"Filing system" means any structures set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria;

"Information officer" in relation to a private body means the head of a private body as contemplated in section 1, of the Promotion of Access to Information Act;

"Information Regulator" means the person appointed as the Information Regulator in terms of section 39 of the POPI Act;

"Management" means all personnel who direct, control, exercise authority over, supervise or oversee the business activities of any area, function, team, role or aspect of Netmed Strand, operations, or business activities, including Executive Management. Management includes any duly mandated management committee as well as both permanent and acting appointees;

"Operator" means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party;

"Person" means a natural person or a juristic person;

"Personal information" means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but limited to-

(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 it if appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person;

"Prescribed" means prescribed by regulation or by a code of conduct;

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

(a) The collection, receipt, recording, collation, storage, updating or modification, retrieval, alteration, consultation or use;
(b) Dissemination by means of transmission, distribution or making available in any other form; or
(c) Merging, linking, as well as restriction, degradation, erasure or destruction of information;

"PAIA" means the Promotion of Access to Information Act 2 of 2000;

"POPI Act" means the Protection of Personal Information Act 4 of 2013;

"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 the public body;

''Private body'' means

(a) a natural person who carries or has carried on any trade, business or profession, but only in such capacity
(b) a partnership which carries or has carried on any trade, business or profession; or
(c) any former or existing juristic person, but excludes a public body;

"Record" means any recorded information-

(a) Regardless of form or medium, including any of the following:

1) Writing on any material;
2) Information produced, recorded or stored by any means of any tape-recorded, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;
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;
4) Book, map, plan, graph or drawing;
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 produced;

(b) In possession or under the control of a responsible party;
(c) Whether or not it was created by a responsible; and
(d) Regardless of when it came into existence;

''Regulator'' means the Information Regulator established in terms of section 39;

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

(a) Identifies the data subject;
(b) Can be used or manipulated by a reasonably foreseeable method to identify the data subject; or
(c) Can be linked by a reasonably foreseeable method to other information that identifies the subject;

And **"re-identified"** has a corresponding meaning;

"Responsible party" means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information;

"Restriction" means to withhold from circulation, use or publication any personal information that forms part of a filing system, but not to delete or destroy such information;

''Special personal information'' means personal information as referred to in section 26;

"Unique identifier" means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

4. SCOPE

This policy is applicable to all Netmed Strand employees.

5. POLICY STATEMENT

5.1 Netmed Strand understands the need for the protection of personal information and the dissemination thereof. In this light, Netmed Strand undertakes to ensure that all information collected is processed, stored and used in accordance with the Protection of Personal Information Act.

5.2 Personal information may only be processed if:

5.2.1 the data subject consents to such processing;

5.2.2 processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party;

5.2.3 processing is necessary to carry out the mandate of Netmed Strand,

5.2.4 processing complies with an obligation imposed by law on the responsible party;

5.2.5 processing protects a legitimate interest.

5.3 The data subject may object to the processing of personal information in the manner prescribed by the POPI Act. Should the data subject object to the processing of personal information, the responsible party may no longer process the information.

5.4 The responsible party will ensure that personal information under its control is processed:

5.4.1 In a fair, lawful and non-excessive manner;

5.4.2 Only with the informed consent of the data subject; and

5.4.3 Only for a specifically defined purpose.

5.5 Personal information may only be collected directly from the data subject unless:

5.5.1 The information has been derived from or is contained in a public record or has been made public by the data subject;

5.5.2 The data subject has consented to the collection of information from another source;

5.5.3 Collection of the information from another source would not prejudice a legitimate interest of the data subject;

5.5.4 The personal information must be collected for a specific purpose and related to a function of the responsible party.

5.6 A data subject, having provided adequate proof of identity, has the right to request a responsible party to confirm, free of charge, whether or not the responsible party holds personal information about the data subject, and request from a responsible party the record or a description of the personal information about the data subject held by the responsible party, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information.

5.7 The procedure for the retention, destruction and protection of the personal information recorded must be done so in the manner stipulated in **"Annexure A"** to this Policy.

5.8 An Information Officer and will be appointed in terms of the POPI Act.

5.9 The Information Officer will be responsible for:

5.9.1 Ensuring the compliance of Netmed Strand with the POPI Act;

5.9.2 Keeping management updated about Netmed Strand's information protection responsibilities under POPI Act. For instance, in the case of a security breach, the Information Officer must inform and advise management of their obligations pursuant to the POPI Act;

5.9.3 Continually analysing privacy regulations and aligning them with Netmed Strand's personal information processing procedures;

5.9.4 Ensuring that POPI Act audits are scheduled and conducted on a regular basis;

5.9.5 Ensuring that Netmed Strand makes it convenient for data subjects who want to update their personal information or submit POPI Act related complaints to Netmed Strand;

5.9.6 Approving any contracts entered into with, product providers, contractors, employees and other third parties which may have an impact on the personal information held by Netmed Strand;

5.9.7 Encouraging compliance with the conditions required for the lawful processing of personal information;

5.9.8 Ensuring that employees and other persons acting on behalf of Netmed Strand are fully aware of the risks associated with the processing of personal information and that they remain informed about Netmed Strand security controls;

5.9.9 Organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of Netmed Strand;

5.9.10 Addressing employees' POPI Act related questions;

5.9.11 Addressing all POPI Act related requests and complaints made by Netmed Strand's data subjects;

5.9.12 Working with the Information Regulator in relation to any ongoing investigations. The Information Officer will therefore act as the contact point for the Information Regulator authority on issues relating to the processing of personal information and will consult with the Information Regulator where appropriate, with regard to any other matter.

5.10 The purpose of a POPI Act audit is to:

5.10.1 Identify the processes used to collect, record, store, disseminate and destroy personal information;

5.10.2 Determine the flow of personal information throughout Netmed Strand;

5.10.3 Redefine the purpose for gathering and processing personal information;

5.10.4 Ensure that the processing parameters are still adequately limited;

5.10.5 Ensure that new data subjects are made aware of the processing of their personal information;

5.10.6 Re-establish the rationale for any further processing where information is received via a third party;

5.10.7 Verify the quality and security of personal information;

5.10.8 Monitor the extent of compliance with the POPI Act and this policy.

5.10.9 Monitor the effectiveness of internal controls established to manage POPI Act related compliance risk;

5.10.10 In performing the POPI Act audit, the Information Officer will liaise with employees in order to identify areas within Netmed Strand's operation that are most vulnerable or susceptible to the unlawful processing of personal information;

5.10.11 The Information Officer will be permitted direct access to and have demonstrable support from employees and Netmed Strand in performing the duties.

5.11 Consideration will be given on an annual basis to the re-appointment or replacement of the Information Officer.

5.12 Once appointed, Netmed Strand will register the Information Officer with the South African Information Regulator established under POPI Act prior to performing his or her duties.

5.13 Netmed Strand will not distribute or share personal information between entities, associated organisations or individuals not directly involved with facilitating the purpose for which the information was originally collected, unless prior consent is obtained from the data subject.

5.14 The details of the **Information Regulator** are as follows:

Postal Address:	**The Information Regulator (South Africa)** **33 Hoofd Street Forum III,** **3rd Floor '** **Braampark, Johannesburg** **P.O Box 31533** **Braamfontein** **Johannesburg, 2017**
Telephone Number:	**010 023 5207**
Fax Number:	**(011) 403-0668**
Complaints email:	**complaints.IR@justice.gov.za**
General enquiries email:	**inforeg@justice.gov.za**

6. APPROVAL

The Policy will be reviewed biennially and presented to the Board for approval whenever a material change is made to the content thereof.

7. RELATED INFORMATION

The Policy should be read in conjunction with the following supporting guidelines:

7.1 Internal Documents:

- Memorandum of Incorporation of Netmed Strand'
- Rules of Netmed Strand
- PAIA Manual

7.2 Regulatory Requirements:

- Protection of Personal Information Act 4 of 2013
- Promotion of Access to Information Act 2 of 2000
- Companies Act 71 of 2008

8. FINANCIAL IMPLICATIONS

The financial implication of the implementation of this policy may include the training required of the Information Officer to carry out his / her function appropriately, and further training to educate employees on the protection of personal information.

9. EXCLUSIONS

There are no exclusions to this Policy.

10. REQUEST FOR DEVIATIONS FROM THIS POLICY

Subject to any other applicable provision, any request to depart from any particular provision(s) of this Policy shall be made in writing and shall be submitted to the Board, who shall have full authority to grant such request, in whole or in part, or to refuse same. Unauthorised deviations from the provisions of this Policy may result in formal disciplinary action.

11. WARNING

Non-compliance with any applicable regulatory requirements through any deliberate or negligent act or omission, including allowing any personnel, either expressly or impliedly, to not comply with applicable regulatory requirements, will be considered serious and will be dealt with in terms of Netmed Strand's disciplinary process and procedures. This does not preclude any other action as may be provided for in law or any applicable regulatory requirement from being taken against the offender/s.

ANNEXURE A

PROCEDURE FOR RETENTION, DESTRUCTION AND PROTECTION OF THE PERSONAL INFORMATION

1. RETENTION OF RECORDS

1.1 Records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected, unless-

1.1.1 The retention of the record is required or authorised by law;
1.1.2 The responsible party reasonably requires the record for lawful purposes related to its functions or activities;
1.1.3 The retention of the record is required by a contract between the parties thereto;
1.1.4 The data subject has consented to the retention of the record.

2. DESTRUCTION OF RECORDS

2.1 A responsible party must destroy or delete a record of personal information or de-identify it as soon as practicable after the responsible party is no longer authorised to retain the record.

2.2 The destruction or deletion of a record of personal information must be done in a manner that prevents its reconstruction in an intelligible form.

2.3 A responsible party must take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary.

3. COLLECTION OF RECORDS

3.1 When collecting personal information, the data subject must be made aware of-

3.1.1 The information being collected and where the information is not collected from the data subject, the source from which it is collected;
3.1.2 The name and address of the responsible party;
3.1.3 The purpose for which the information is being collected;
3.1.4 Whether or not the supply of the information by that data subject is voluntary or mandatory;
3.1.5 The consequences of failure to provide the information;
3.1.6 Any particular law or requiring the collection of the information;
3.1.7 Any information such as the-

3.1.7.1 Recipient or category of recipients of the information;
3.1.7.2 Nature or category of recipients to the information;
3.1.7.3 Existence of the right to object to the processing of personal information and;
3.1.7.4 The right to lodge complaint to the Information Regulator and the contact details of the Information Regulator, which is necessary, having regard to the specific circumstances in which the information is or is not to be processed, to enable processing in respect of the data subject to be reasonable.

4. SECURITY OF INFORMATION

4.1 A responsible party 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-

4.1.1 Loss of, damage to or unauthorised destruction of personal information; and
4.1.2 Unlawful access to or processing of personal information.

4.2 The responsible party must take reasonable measures to-

4.2.1 Identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;
4.2.2 Establish and maintain appropriate safeguards against the risks identified;

4.2.3 Regularly verify that the safeguards are effectively implemented; and
4.2.4 Ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

4.3 The responsible party must have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms specific industry rules and regulations.

4.4 Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the responsible party must notify the Information Regulator and the data subject, unless the identity of such data subject cannot be established.

4.5 Such notification must be made as soon as reasonably possible after the discovery of the compromise, taking into account 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 responsible party's information system.

4.6 The responsible party may only delay notification of 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 concerned.

4.7 The notification to a data subject must be in writing and communicated to the data subject in at least one of the following ways:

4.7.1 Mailed to the data subject's last known physical or postal address;
4.7.2 sent by e-mail to the data subject's last known e-mail address;
4.7.3 placed in a prominent position on the website of the responsible party;
4.7.4 published in the news media; or
4.7.5 as may be directed by the Regulator.

4.8 The notification must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including:

4.8.1 a description of the possible consequences of the security compromise;
4.8.2 a description of the measures that the responsible party intends to take or has taken to address the security compromise;
4.8.3 a recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and
4.8.4 the identity of the unauthorised person who may have accessed or acquired the personal information, if known to the responsible party.

5. Netmed Strand must, in conjunction with its ICT consultant / service provider:

5.1 Ensure that Netmed Strand' ICT infrastructure, filing systems and any other devices used for processing personal information meet acceptable security standards;

5.2 Ensure that all electronically held personal information is kept only on designated drives and servers and uploaded only to approved cloud computing services;

5.3 Ensure that servers containing personal information are sited in a secure location, away from the general office space;

5.4 Ensure that all electronically stored personal information is backed-up and tested on a regular basis;

5.5 Ensure that all back-ups containing personal information are protected from unauthorised access, accidental deletion and malicious shacking attempts;

5.6 Ensure that personal information being transferred electronically is encrypted;

5.7 Ensure that all servers and computers containing personal information are protected by a firewall and the latest security software;

5.8 Perform regular IT audits to ensure that the security of Netmed Strand's hardware and software systems are functioning properly;

5.9 Perform regular IT audits to verify whether electronically stored personal information has been accessed or acquired by any unauthorised persons;

5.10 Performing a proper due diligence review prior to contracting with operators or any other third-party service providers to process personal information on Netmed Strand's behalf.

ANNEXURE B

POPI COMPLAINT PROCEDURE

1. Data subjects have the right to complain in instances where any of their rights under the POPI Act have been infringed upon. Netmed Strand takes all complaints very seriously and will address all POPI Act related complaints in accordance with the following procedure:

1.1 POPI Act complaints must be submitted to Netmed Strand in writing. Where so required, the Information Officer will provide the data subject with a "POPI Complaint Form". Where the complaint has been received by any person other than the Information Officer, that person will ensure that the full details of the complaint reach the Information Officer within 1 working day.

1.2 The Information Officer will provide the complainant with a written acknowledgement of receipt of the complaint within 2 working days.

1.3 The Information Officer will carefully consider the complaint and address the complainant's concerns in an amicable manner. In considering the complaint, the Information Officer will endeavour to resolve the complaint in a fair manner and in accordance with the principles outlined in the POPI Act.

1.4 The Information Officer must also determine whether the complaint relates to an error or breach of confidentiality that has occurred and which may have a wider impact on the Netmed Strand's data subjects.

1.5 Where the Information Officer has reason to believe that the personal information of data subjects has been accessed or acquired by an unauthorised person, the Information Officer will consult with Netmed Strand, where after the affected data subjects and the Information Regulator will be informed of this breach.

1.6 The Information Officer will revert to the complainant with a proposed solution with the option of escalating the complaint to Netmed Strand within 7 working days of receipt of the complaint. In all instances, Netmed Strand will provide reasons for any decisions taken and communicate any anticipated deviation from the specified timelines.

1.7 The Information Officer's response to the data subject may comprise any of the following:

1.7.1 A suggested remedy for the complaint;
1.7.2 A dismissal of the complaint and the reasons as to why it was dismissed;
1.7.3 An apology (if applicable) and any disciplinary action that has been taken against any employees involved.

1.8 Where the data subject is not satisfied with the Information Officer's suggested remedies, the data subject has the right to complain to the Information Regulator.

1.9 The Information Officer will review the complaints process to assess the effectiveness of the procedure on a periodic basis and to improve the procedure where it is found wanting. The reason for any complaints will also be reviewed to ensure the avoidance of occurrences giving rise to POPI Act related complaints

POPI COMPLAINT FORM

We are committed to safeguarding your privacy and the confidentiality of your personal information and are bound by the Protection of Personal Information Act.

Please submit your complaint to the POPI Information Officer:	
Name:	**Dr Josias Coetsee**
Contact number:	**021 853 6903**
E-mail address:	financial@netmed.co.za

If we are unable to resolve your complaint to your satisfaction, you have the right to submit a complaint to the **Information Regulator**:

33 Hoofd Street
Forum III 3rd Floor
Braampark
Braamfontein
Johannesburg

Email: inforeg@justice.gov.za
Complaints: complaints.IR@justice.gov.za
Website: https://www.justice.gov.za/inforeg/index.html

A. Particulars of Complainant:	
Name and Surname:	
Identity Number:	
Postal Address:	
Contact Number:	
E-mail Address:	
B. Details of complaint:	
C. Desired Outcome:	
D. Signature	
Signature:	
Date:	