VALOMATE

MEDICAL SERVICES

DATA PRIVACY POLICY

1. Introduction and Purpose

1.1 Valomate Medical Services (Pty) Ltd ("Valomate") is a service provider to supplier claimants of the road accident fund. Valomate, working with EMS providers, private hospitals and medical specialists, facilitates the medical treatment of victims of road accidents both in emergency situations and via the patient's undertaking issued by the Road Accident Fund some years after their accident.

1.2 As part of managing the business and creating value for its various stakeholders, Valomate is required to process personal information. Accordingly, Valomate is obligated to comply with The Protection of Personal Information Act 4 of 2013 ("POPIA/The Act") insofar as it processes personal information, including special personal information, during its ordinary course of business. Under POPIA, Valomate is defined as the Responsible Party for all Personal Information it processes.

1.3 Valomate is also obligated to comply with the National Health Act No 61 of 2003 (NHA); the Road Accident Funds Act No 56 of 1996 (RAF Act); and the Promotion of Access to Information Act No 2 of 2000 (PAIA).

1.4 Valomate guarantees its commitment to protecting the data subjects privacy, ensuring that their personal information is processed appropriately, securely and in accordance with all applicable legislation, both within South Africa and outside of it.

1.5 This Policy sets out the manner in which Valomate processes personal information and stipulates the purpose for which said information is used, specifically addressing:

1.5.1 Types of Personal Information Valomate collects on a Data Subject and the basis thereof
1.5.2 The use and protection of the Personal Information of a Data Subject
1.5.3 Retention periods of the Personal Information of a Data Subject
1.5.4 The rights of a Data Subject regarding their Personal Information
1.5.5 The process the Data Subject should follow if he does not want to provide Valomate with his personal information.

2. Scope

This policy applies to all the Personal Information Valomate processes in the ordinary course of business but does not deal in detail with the Personal Information of employees, consultants and contractors which is the subject of a different policy (The Employee Data Privacy Policy).

3. Background

3.1 Data Protection Legislation applies to information relating to identifiable individuals and juristic persons (collectively referred to as Data Subjects), in terms of the Protection of Personal Information Act 4 of 2013 (POPIA).

3.2 The purpose of POPIA is to give effect to the constitutional right to privacy, by safeguarding personal information when processed by a responsible party, in order to:

3.2.1 Balance the right to privacy against other rights, particularly the right of access to information

3.2.2 Regulate the way in which Personal Information may be processed, by establishing conditions which prescribe the minimum requirements for the lawful processing of personal information.

3.3 POPIA provides Data Subjects with measurable rights and remedies to protect their personal information from processing which is not in accordance with the Act.

4. Policy Statement

Valomate is committed to following best practice; to aligning with the principles of good governance and to adhering to legislative compliance requirements in all aspects of our business.

Valomate guarantees its commitment to protecting the data subject's privacy and ensuring their Personal information and Special Personal Information is processed in accordance with all applicable legislation relevant to our industry.

As the Responsible Party, Valomate processes Personal Information in accordance with the requirements of the Protection of Personal Information Act, 2013 (POPIA).

This Policy must be read in conjunction with POPIA and its Regulations, where applicable.

5. Definitions

In this policy:

5.1 Clause headings are for convenience and reference only and shall not be used in the interpretation thereof

5.2 Any gender includes the other genders and a natural person includes a juristic person and vice versa

5.3 All the annexures (if any) hereto are incorporated herein and shall have the same force and effect as if they were set out in the body of this policy

5.4 The following words and/or expressions shall, unless the context indicates otherwise, bear the meaning assigned to them below and in POPIA

5.4.1 *Data Subject* means the person to whom personal information relates

5.4.2 *Child* means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning himself. A child is afforded special protection under POPIA in relation to the lawful processing of his information

5.4.3 *Competent Person* is any person who is legally competent to consent to any action or decision in respect of a Child, i.e. a Child's parent or legal guardian;

5.4.4 *POPIA* refers to the Protection of Personal Information Act 4 of 2013;

5.4.5 *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. Called Controllers in other jurisdictions (GDPR)

5.4.6 *Operator* means a person who is contracted to process personal information on behalf of the responsible party but is not controlled by the Responsible Party.

5.4.7 *Processing* means any operation or activity, whether by automatic means or not, concerning personal information, including:

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

5.4.8 *Record* means any recorded information

a) Regardless of form or medium, including any of the following:
    i) Writing of any material
    ii) 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

iii) Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means
iv) Book, map, plan, graph or drawing
v) Photograph, film, negative, tape or other device in which one or more visual images are embodied to be capable, with or without the aid of some other equipment, of being reproduced, in the possession or under the control of a responsible party

b) Whether or not it was created by a responsible party and
c) Regardless of when it came into existence.

5.4.9 *Personal Information* means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to

a) Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, wellbeing, 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 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
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

5.4.10 *Special Personal Information* refers to the personal information concerning the following: the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject.

5.4.11 *De-identify* means to delete any information which identifies the data subject; can be used or manipulated by a reasonably foreseeable method to identify the data subject; or can be linked by a reasonably foreseeable method to other information that identifies the data subject.

5.4.12 *Consent* is defined as the voluntary, specific and informed expression of will in terms of which permission is granted for the Processing of Personal Information;

5.4.13 *Medical Service Providers (MSP's)* means Emergency Medical Service providers, Private Hospitals and Medical Specialists.

5.4.14 *Road Accident Fund (RAF)* means the South African state insurer responsible for providing compulsory insurance cover to all users of South African roads; to rehabilitate and compensate persons injured as a result of the negligent driving of motor vehicles and to promote road safety in South Africa.

6. Data Subject Rights

All Data Subjects have the following rights, which Valomate is committed to uphold. The practical implementation of this policy will be in alignment with these rights as well as the principles of lawful processing as set out in POPIA (Section 5)

6.1 Objection to the use of Personal Information on reasonable grounds relating to his situation

6.2 Notification if:
- 6.2.1 Information is being collected
- 6.2.2 Information is being used for something other than the original purpose for which consent was given
- 6.2.3 Information has been accessed or acquired by an unauthorised person

6.3 Establishing whether the responsible party holds Personal Information and to request, in a format legible and readable, access to said information

6.4 Requesting that Personal Information be corrected, destructed or deleted

6.5 Refusing processing for direct marketing by unsolicited electronic communications

6.6 Lodging a complaint with the Information Regulator

6.7 Instituting civil proceedings against a party who has acted unlawfully in relation to the Data Subjects Personal Information (Sec 99)

7. Conditions for Lawful Processing

Valomate undertakes to adhere to the 8 Conditions for Lawful Procession of Personal Information as set out in POPIA (Sections 8-35):

7.1 Accountability

Valomate accepts full responsibility and accountability to responsibly manage and protect all the Personal Information we process

7.2 Processing Limitation

7.2.1 Valomate will, wherever reasonably possible, collect information directly from the Data Subject, unless collection from another party is specifically permitted; the data subject has consented and the collection of information from a third party will not prejudice the data subject:

a) In the case of Patient data, regarding a child or mentally incompetent adult, where a competent adult provides information on their behalf
b) In the case of medical history, information will be collected from the Medical Service Provider/s

7.2.2 Wherever reasonably possible, Data subjects express consent will be obtained. In the event that they are unable to consent due to the nature of their injuries, or status as a minor, consent will be sought from their next of kin/competent person. In the rare case where no consent can be obtained, Valomate will proceed on the principle of furthering the legitimate interests of the Data Subject.

7.2.3 All Personal Information is processed to:

a) Protect the legitimate interest of data subject: in this case to protect their right to access quality medical care
b) Pursue the legitimate interest of Valomate and the MSP providing the care.

7.2.4 We respect the right of the Data Subject to, at any time, object or withdraw consent to any further processing and we have procedures in place for these instances

7.3 Purpose Specification

7.3.1 Valomate will collect and process the absolute minimum data reasonably required in order to submit the claim to the RAF:

7.3.1.1 This data will be that which is stipulated by the RAF in their submission documentation

7.3.1.2 This data does fall into the category of Special Personal Information, as it includes the Data Subjects race, as well as details of their medical treatment and medical history. This information is collected only insofar as it is required by the RAF for the submission of claim documents, and processing of this Personal Information is necessary for the establishment, exercise or defence of a right or a claim, as required by POPIA.

7.3.2 Valomate will only process Personal Information which is essential to enable us to fund medical treatment provided to accident victims, and to complete the claim process against the RAF

7.3.3 The Data Subject will be made aware of the purpose of the collection through their consent form signed before treatment commences.

7.3.4 We shall only retain and store Personal Information for the period for which the data is required to serve its primary purpose or a legitimate interest or for the period required to comply with an applicable legal requirement, whichever is longer.

7.3.4.1 All records will be de-identified and/or destroyed at the time dictated by POPIA and other relevant governing legislation (National Health Act 61 of 2003; the Road Accident Funds Act 56 of 1996; the Promotion of Access to Information Act 2 of 2000; and the Children's Act 38 of 2005). Please see Record Retention Policy for further information.

7.3.4.2 Personal Information will be destroyed, deleted or de-identified as soon as is reasonably practical, preventing its reconstruction in an intelligible form.

7.4 Further Processing Limitation

7.4.1 Valomate will ensure that any further processing will be in accordance or compatible with the purpose for which it was originally collected, and will not take place without the express consent of the Data Subject.

7.4.2 The Information Officer shall ensure that the information collected will not be used for any other purpose before obtaining the individual's approval, unless the new purpose is required by law

7.4.3 Valomate will not share any Personal Information with anyone or for any reason if not required for the finalization of the claim, or as required in terms of legislation or regulations

7.5 Information Quality

7.5.1 Reasonably practicable steps will be taken to ensure that the Personal Information is complete, accurate, not misleading and that the Personal Information is updated where necessary

7.5.2 In actioning the above, Valomate will regularly review the purpose for which personal information is collected or further processed.

7.6 Openness

Valomate will take reasonably practicable steps to be open and transparent on the nature, extent and reasons for processing Personal Information

To that end, we will ensure, through the use of a consent form, that the Data Subject is aware of:

7.6.1 The information being collected
7.6.2 Our name and address
7.6.3 The purpose for which the information is being collected
7.6.4 Whether or not the supply of the information is voluntary or mandatory
7.6.5 The consequences of failure to provide the information
7.6.6 The right of access to and the right to rectify the information collected
7.6.7 The right to object to the processing of the information

The Information Officer shall also ensure that a person collecting Personal Information will be able to explain to the individual why this is being done: this will involve adequate training of all staff and MSP Partners

7.7 Security Safeguards

7.7.1 Valomate will adequately safeguard and protect all Personal Information in our possession by adopting the appropriate, reasonable technical organisational measures expected for our industry and within South Africa

7.7.2 We will, on an ongoing basis, continue to review our security controls and related processes to ensure that all Personal Information we hold remains secure

7.7.3 Generally accepted standards of technology and operational security have been implemented to protect information from loss, misuse, alteration, or destruction.

The Physical Security Measures include, but are not limited to:

a) Physical barriers to entry to the premises, according to generally accepted South African norm: locked doors, security gates, alarm system, electric fencing, 24-hour security guards on site
b) Key-card access for all internal lifts and office doors
c) Physical locks on all internal doors
d) Locks on all filing cabinets and desk drawers
e) Kensington locks on all computers
f) No laptops for any staff except the executive team

The IT security measures include, but are not limited to:

g) Adequate password and passphrase protection on every device, system and sensitive document, governed by the Password Policy which all staff will be trained on
h) High quality antivirus software on all devices
i) Virtualisation/ Containerisation
j) All data backed up to secure servers under Valomate's control
k) A comprehensive Data Recovery Plan
l) Staff training to avoid phishing scams, and email warnings on all outside emails
m) A protocol to always maintain updated software
n) Centralised end-point security
o) A comprehensive Information Security and IT Change Management Policy

7.7.4 All our employees are trained on information security and are required to keep Personal Information confidential and only authorised persons have access to such information.

7.7.5 Any Operator processing information on behalf of Valomate will be required to sign a Non-Disclosure agreement and an Operator Agreement in order to ensure:

7.7.5.1 Information is treated as confidential and not disclosed required by POPIA

7.7.5.2 They apply at least the same security measures as Valomate

7.7.6 The Information Officer shall ensure that all employees, consultants and contractors have signed Non-Disclosure Agreements and have been adequately trained on the contents of this Policy, and other relevant Policies and Procedure Manuals.

7.7.7 The Information Officer shall ensure that care is taken when personal information is disposed of or destroyed to prevent unauthorized parties from gaining access to it.

7.7.8 Valomate will notify data subject and the Regulator of any breach of data.

7.8 Data Subject Participation

7.8.1 Valomate commits to freely confirm what Personal Information we hold on Data Subjects, to update and rectify the Personal Information upon request and to keep it for no longer than required.

7.8.2 We respect that the Data Subject may request us to:

7.8.2.1 Correct or delete information, which is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully

7.8.2.2 Delete or destroy information that we are no longer authorised to retain

7.8.3 We will not use Personal Information for any other purpose than that set out in this Policy, and we will take the necessary steps to secure the integrity and confidentiality of Personal Information in our possession and under our control by taking appropriate and reasonable measures to prevent loss of, damage to or unauthorised destruction of Personal Information and to prevent the unlawful access to, or processing of Personal Information.

8. Personal Information Processed

8.1 Information is processed in order to:

8.1.1 Fund the private medical treatment of non-medical aid patients, including children, where the Medical Service Provider will have a valid Supplier Claim against the Road Accident Fund.

8.1.2 Submit this claim, on behalf of the Medical Service Provider/s, to the Road Accident Fund .

8.1.3 Valomate, therefore, holds information on both Patients and the Medical Service Providers who have treated them.

8.2 The Patient Personal Information:

8.2.1 General Personal Information

a) Name
b) ID Number
c) Date of Birth and Age
d) Gender
e) Race
f) Nationality
g) Contact Details (Email; Telephone Number)

8.2.2 Accident Details

a) Accident Date
b) AR Number
c) Case Number
d) Accident Location
e) SAPS Station
f) Accident Type
g) Transferred By

8.2.3 Admission Details

a) Admission Date
b) Suspected Injury
c) Supplier
d) Level of Care
e) Admitting Physician

8.2.4 Medical Details

a) Blood Pressure
b) Pulse
c) Temperature
d) GCS
e) Comorbidities

8.2.5 Full Medical File

a) Details of Injuries
b) Procedures and Surgeries performed
c) Duration of hospital stay
d) Treatment and recovery plans
e) Names of treating Doctors and Medical Specialists

8.3 The Medical Service Provider Personal:

8.3.1 Company Name
8.3.2 Company Registration Number
8.3.3 Names of Contact Persons on Staff (Head Office and individual hospitals, clinics, branches)
8.3.4 Physical Addresses
8.3.5 Postal Address
8.3.6 Cellphone Numbers and Email Addresses of Contact Persons
8.3.7 Financial information including invoices and statements
8.3.8 Practice Numbers
8.3.9 Bank details

8.4 All the above Personal Information is processed in order to:

8.4.1 Approve the payment for medical treatment needed
8.4.2 To complete the required documentation for submission to the Road Accident Fund.
8.4.3 To respond to queries from MSP's and Patients
8.4.4 To confirm and verify a Patients' identity
8.4.5 To comply with all legislative or regulatory requirements related to services provided by us

8.4.6 To satisfy any requirement by a professional body or network to which we are a member

8.4.7 To fulfil our contractual obligations to the Medical Service Providers, for example to ensure that invoices are issued correctly, to communicate and to carry out instructions and requests

8.4.8 In connection with possible requirements by the Information Regulator or other Government agencies allowed by law, legal proceedings, or court rulings.

9. Storage and Access

9.1 Information is stored on OneDrive and the private data and business management system curated by Valomate and available for its exclusive use.

9.2 Information is accessible only to Valomate staff and Operators who have a verifiable need to access the information in order to meet an objective/requirement of either the organization or the data subject.

9.3 Any physical sources of data are scanned in and stored electronically, and the original hard copy is, wherever permitted by legislation, destroyed.

9.4 Where a hard copy needs to be kept, it is kept in a locked, fireproof filing cabinet to which only the CEO has access.

9.5 Data is stored on secure servers owned and managed by compliant operators, with whom Valomate has signed NDA's, SLA's and privacy agreements.

9.6 All electronic files or data are backed up by the IT Service Provider who is also responsible for system security which protects third party access and physical threats. Please see Information Security Policy for further details.

9.7 Information is only processed in so far as it is necessary to fulfil the requirements of the data subject or to meet a need of the Responsible Party.

9.8 A Security Incident Management Register will be kept to log any security incidents.

10. The Sharing and Transfer of Personal Information

Our employees will have access to Personal Information to administer and manage our services and internal business processes.
We do not share Personal Information with third parties unless we have a lawful basis for doing so:

10.1 Valomate shares Personal Information it has collected from the Medical Service Providers with the Road Accident Fund in the furtherance of its legitimate interest to pursue a claim against the fund on behalf of the Medical Service Provider.

10.2 Valomate will never disclose any of the Personal Information it collects to any other third parties, unless:

10.2.1 The sharing of the information is essential in order to fulfil a need of the Data Subject, but will only be shared in this instance with express consent of the data subject.

10.2.2 We have a duty or a right to disclose in terms of legislation, regulations or industry codes

10.2.3 We believe it is necessary to protect our rights

10.2.4 Explicitly requested by the Data Subject;

10.3 At this stage we do not have the need to share Personal Information outside of South Africa. If ever a legitimate need for cross-border data transfer to arise, it will only be done in very limited circumstances and in strict adherence to all requirements of POPIA and other relevant legislation (Section 72).

11. Information Officer Responsibilities

Valomate has appointed an Information Officer and will ensure the Information Officer is aware of the IO Core Focus/Duties under POPIA, which include, as per POPIA (Section 55)

11.1 Encouraging compliance with the information protection conditions in terms of Section 55 of POPIA.

11.2 Developing, publishing and maintaining this Privacy Policy which addresses all relevant provisions of POPIA.

11.3 Reviewing POPIA and periodic updates as published.

11.4 Ensuring that POPIA induction training takes place for all staff.

11.5 Ensuring that periodic communication awareness on POPIA responsibilities takes place.

11.6 Ensuring that Privacy Notices for internal and external purposes are developed and published.

11.7 Handling data subject access requests.

11.8 Approving contracts with Data Operators.

11.9 Ensuring that appropriate policies and controls are in place for ensuring the quality of Personal Information.

11.10 Ensuring that appropriate Security Safeguards are in place.

11.11 Considering requests made pursuant to POPIA.

11.12 Working with the Regulator in relation to investigations conducted pursuant to Chapter 6 against Valomate.

11.13 Identifying and governing all privacy related risks.

11.14 Mapping all activities performed concerning the collection and storage of personal information i.e., before and post enactment of POPIA.
11.15 Mapping all privacy laws and industry codes relevant to our activities.
11.16 Coordinating the development, implementation, and maintenance of corporate customer (external) and employee (internal) privacy policies.
11.17 Ensuring compliance with corporate privacy policies and procedures.
11.18 Liaising with Human Resources and Legal Departments to ensure standards of disciplinary action and sanctions for non-compliance.
11.19 Liaising with Public Relations and Marketing Departments to create public information communications and procedures on privacy efforts, related issues and breaches.
11.20 Creating standards or scripts for responding to customer or public enquiries.
11.21 Creating and implementing procedures and standards to facilitate customer verification of captured and stored personal information files.
11.22 Monitoring and controlling the privacy requirements and responsibilities of information processing service providers or operators in terms of sections 20 and 21 of POPIA.
11.23 Managing breach and incident investigation processes.
11.24 Creating and implementing our privacy breach management plan, privacy alerts, and other privacy related operational issues.
11.25 Creating standards and procedures to manage any compromise in the security of the stored personal information correctly and appropriately.
11.26 Investigating, analysing and documenting all privacy related incidents and complaints.
11.27 Applying investigation findings to update standards, processes and systems as an on-going operational improvement routine.

The Information Officer is Bianca Van Zyl whose details are available below and who is responsible for compliance with the conditions of the lawful processing of personal information and other provisions of POPIA.

12. Supplementary Policies

Additional Policies, relevant to Privacy and POPIA, and expanding on the topics contained herein:

12.1 PAIA Policy
12.2 Privacy Statement
12.3 Information Security Policy
12.4 IT Change Management Policy
12.5 Financial Data Policy
12.6 Employee Data Privacy Policy
12.7 Employee Exit Policy
12.8 Record Retention Policy
12.9 Incident Response Policy
12.10 Complaints Policy
12.11 Clean Desk Policy

12.12 Password Policy

13. Staff Training and Acceptance

13.1 This Policy has been implemented throughout Valomate and comprehensive team training on this policy and POPIA has been completed.

13.2 The documentation for staff is contained in this policy document and other materials made available by the Information Officer. The Information Officer will ensure that all staff with access to any kind of personal information will have their responsibilities outlined during their induction procedures.

13.3 Ongoing programmes will provide opportunities for staff to explore POPIA issues through training, team meetings, and supervisions.

13.4 Each new employee will be required to sign an Employment Contract containing relevant clauses for the use and storage of employee information, or any other action so required, in terms of POPIA

13.5 Every employee currently employed by Valomate has been required to sign an addendum to their Employment Contracts containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPIA.

13.6 The Information Officer will ensure that all staff sign acceptance of this policy once they have had a chance to understand it, as well as their responsibilities in terms of the policy and POPIA.

14. Policy Review.

14.1 The Information Officer is responsible for an annual review to be completed prior to the policy anniversary date.

14.2 The Information Officer will ensure relevant stakeholders are consulted as part of the annual review to be completed prior to the policy anniversary date.

14.3 This policy shall also be reviewed whenever:

14.3.1 There have been changes in International, National or Internal references that may impact on this policy.

14.3.2 There are improvements or changes within the Valomate systems or processes which should be reflected in this policy.

15. Details of Information Officer

Information Officer Details Name: Bianca Van Zyl
Postal Address: 16 First Street, Menlo Park, Pretoria
Email Address: popia@valomatemedical.co.za

16. Recourse

If you have an inquiry or complaint regarding this Policy or the collection or use of your Personal Information, including any rights of access, ability to limit the use or disclosure of Personal Information, or to correct or delete inaccurate Personal Information, please email popia@valomatemedical.co.za.

If the Data Subject is not satisfied with the response, Valomate acknowledges the Data Subjects right under POPIA to lodge a complaint directly with the Information Regulator, and will direct the Data Subject to this in the Complaints Policy.

The Information Regulator (South Africa) is an independent body established in terms of Section 39 of the POPIA of 2013. It is, among other things, empowered to monitor and enforce compliance by public and private bodies, and is subject only to the constitution and accountable to the National Assembly.