



PROTECTION OF PERSONAL INFORMATION POLICY

FOR

MEDICAL FORUM THEATRE

Table of Contents

1. INTRODUCTION:	4
2. DEFINITIONS:	4
2.1 Person:	4
2.2 Personal Information:	4
2.3 Data Subject:	5
2.4 Responsible Party:	5
2.5 Operator:	5
2.6 Information Officer:	5
2.7 Processing:	5
2.8 Record:	5
2.9 Filing System:	6
2.10 Unique Identifier:	6
2.11 De-Identify:	6
2.12 Re- Identify:	6
2.13 Consent:	6
2.14 Direct Marketing:	7
2.15 Biometrics:	7
2.16 Binding Corporate Rules:	7
3. POLICY PURPOSE:	7
4. MEDICAL FORUM THEATRE COMMITMENT:	8
5. POLICY APPLICATION:	8
6. LEGISLATIVE FRAMEWORK:	9
7. RIGHTS OF DATA SUBJECTS:	9
8. GENERAL GUIDING PRINCIPLES:	10
9. INFORMATION OFFICERS:	13
10. SPECIFIC DUTIES AND RESPONSIBILITIES:	14
11. POPI AUDIT:	18
12. REQUEST TO ACCESS PERSONAL INFORMATION PROCEDURE:	19
13. POPI COMPLIANTS PROCEDURE:	19
14. DISCIPLINARY ACTION:	20

15. RETENTION AND RESTRICTION OF DOCUMENTS:.....	20
16. SECURITY COMPROMISES:	22
17. POINT OF CONTACT:	22
18. REVIEW OF POLICY:.....	23

1. INTRODUCTION:

The right to privacy is an integral human right recognised and protected in the South African Constitution and in the Protection of Personal Information Act 4 of 2013 (“POPIA”).

POPIA 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.

Medical Forum Theatre is involved in the collection, use and disclosure of certain aspects of the personal information of patients, employees and other stakeholders.

Given the importance of privacy, Medical Forum Theatre is committed to effectively managing personal information in accordance with POPIA’s provisions.

POPIA is not intended to prevent the processing of personal information but to ensure that it is done fairly and without adversely affecting the rights of data subjects.

Medical Forum Theatre guarantees its commitment to protecting its data subjects’ privacy and ensuring that their personal information is used appropriately, transparently, securely and in accordance with applicable laws.

2. DEFINITIONS:

2.1 Person:

Means a natural person or a juristic person.

2.2 Personal Information:

Personal information is any information that can be used to reveal a person’s identity.

Personal Information relates to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person (such as a company), including, but not limited to information concerning:

- Race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person;
- Information relating to the education or medical, financial, criminal or employment history of the person;
- Any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
- The biometric information of the person;
- The personal opinions, views or preferences of the person;

- Correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- Views or opinions of another individual about the person;
- 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.

2.3 Data Subject:

This refers to the natural or juristic person to whom personal information relates.

2.4 Responsible Party:

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.

2.5 Operator:

An 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.

2.6 Information Officer:

The Information Officer is responsible for ensuring Medical Forum Theatre's compliance with POPIA.

Once appointed, the Information Officer must be registered with the Information Regulator established under POPIA prior to performing his/ her or its duties.

2.7 Processing:

The Act of Processing information includes any activity or any set of operations, whether or not by automatic means, concerning information and includes:

- The collection, use, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
- dissemination by means of transmission, distribution or making available in any other form; or
- merging, linking, as well as any restriction, degradation, erasure or destruction of information.

2.8 Record:

Means any recorded information –

- (a) Regardless of form or medium, including any of the following:
 - Writing on any material;

- Information produced, recorded or stored by 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;
 - Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
 - Book, map, plan, graph or drawing;
 - Photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;
- (b) In the possession or under control of a responsible party;
- (c) Whether or not it was created by a responsible party; and
- (d) Regardless of when it came into existence.

2.9 Filing System:

Means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria.

2.10 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.

2.11 De-Identify:

This means to delete any information that identifies a data subject or which can be used by a reasonably foreseeable method to identify, or when linked to other information, that identifies the data subject.

2.12 Re- Identify:

In relation to personal information of a data subject, means to resurrect any information that has been de-identified that identifies the data subject, or can be used or manipulated by a reasonably foreseeable method to identify the data subject.

2.13 Consent:

Means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.

2.14 Direct Marketing:

Means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of:

- (a) Promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or
- (b) Requesting the data subjects to make a donation of any kind for any reason.

2.15 Biometrics:

Means a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprints, DNA analysis, retinal scanning and voice recognition.

2.16 Binding Corporate Rules:

Means personal information processing policies, within a group of undertakings, which are adhered to by Medical Forum Theatre or operation within that group of undertakings when transferring personal information to a business or operator within that same group.

3. POLICY PURPOSE:

The purpose of this policy is to protect Medical Forum Theatre from the compliance risks associated with the protection of personal information which includes:

- Breaches of Confidentiality where Medical Forum Theatre could suffer loss in revenue where it is found that the personal information of data subjects has been shared or disclosed inappropriately.
- Failing to offer a choice, including the choice where all data subjects should be free to decide how and for what purpose Medical Forum Theatre uses information relating to them.
- Reputational Damage: Medical Forum Theatre could suffer a decline in shareholder value following an adverse event such as a computer hacker deleting the personal information held by Medical Forum Theatre.

4. MEDICAL FORUM THEATRE COMMITMENT:

This policy demonstrates the Medical Forum Theatre's commitment to protecting the privacy rights of data subjects in the following manner:

- Through stating desired behaviour and directing compliance with the provisions of POPIA and best practice.
- By cultivating a culture that recognises privacy as a valuable human right.
- By developing and implementing internal controls for the purpose of managing the compliance risk associated with the protection of personal information.
- 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 Medical Forum Theatre.
- By assigning specific duties and responsibilities to employees, including the appointment of an Information Officer and Deputy Information Officer/s in order to protect the interest of Medical Forum Theatre and data subjects.
- By raising awareness through training and providing guidance to individuals who process personal information so that they can act confidently and consistently.

5. POLICY APPLICATION:

Medical Forum Theatre and its employees shall adhere to this policy in the handling of all personal information received from, but not limited to natural persons, employees, patients, suppliers, agents, representatives and business partners to ensure compliance with this Act, applicable regulations and other rules relating to the protection of personal information.

The policy's guiding principles find application in all situations and must be read in conjunction with POPIA as well as Medical Forum Theatre's PAIA Policy as required by the Promotion of Access to Information Act (Act No 2 of 2000).

The legal duty to comply with POPIA's provisions is activated in any situation where there is a processing of personal information which is entered into a record by or for a responsible person who is domiciled in South Africa.

POPIA does not apply in situations where the processing of personal information:

- Is included in the course of purely personal or household activities; or
- Where the personal information has been de-identified.

6. LEGISLATIVE FRAMEWORK:

- Constitution of the Republic of South Africa, Act 108 of 1996
- The Protection of Personal Information Act no 4 of 2013, as amended
- Basic Conditions of Employment Act, 75 of 1997
- Broad Based Black Economic Empowerment Act, 53 of 2003
- Employment Equity Act, 55 of 1998
- Labour Relations Act 66 of 1995, as amended
- Skills Development Levies Act, 9 of 1999
- Electronic Communications and Transaction Act, 25 of 2002
- National Health Act, 61 of 2003

7. RIGHTS OF DATA SUBJECTS:

Where appropriate, Medical Forum Theatre will ensure that its data subjects are made aware of the rights conferred upon them.

Medical Forum Theatre will ensure that it gives effect to the following seven rights:

7.1 The Right to Access Personal Information:

Medical Forum Theatre recognises that a data subject has the right to establish whether Medical Forum Theatre holds personal information relating to him, her or it including the right to request access to that personal information.

If a data subject searches for a record and it is believed that the record either does not exist or cannot be found, the requester will be notified by way of an affidavit or affirmation. This will include steps that were taken to attempt to locate the record.

7.2 The Right to have Personal Information Corrected or Deleted:

The data subject has the right to request, where necessary, that his, her or its personal information must be corrected or deleted where Medical Forum Theatre is no longer authorised to retain the personal information.

7.3 The Right to Object to the Processing of Personal Information:

The data subject has the right, on reasonable grounds, to object to the processing of his, her or its personal information.

In such circumstances, Medical Forum Theatre will give due consideration to the request and requirements of POPIA.

Medical Forum Theatre, may cease to use or disclose the data subject's personal information and may, subject to any statutory and contractual record keeping requirements, also approve the destruction of the personal information.

7.4 The Rights to Object to Direct Marketing:

The data subject has the right to object to the processing of his, her or its personal information for purposes of direct marketing by means of unsolicited electronic communications.

7.5 The Right to Complain to the Information Regulator:

The data subject has the right to submit a complaint to the Information Regulator regarding an alleged infringement of any of the rights protected under POPIA and to institute civil proceedings regarding the alleged non-compliance with the protection of his, her or its personal information.

The data subject also has the right to be notified in any situation where Medical Forum Theatre has reasonable grounds to believe that personal information of the data subject has been accessed or acquired by an unauthorised person.

8. GENERAL GUIDING PRINCIPLES:

All Employees and persons acting on behalf of Medical Forum Theatre will at all times be subject to, and act in accordance with, the following guiding principles:

8.1 Accountability:

Medical Forum Theatre must ensure that the conditions set out in the Act, and all measures that give effect to such conditions, are complied with at the time of the determination of the purposes and means of the processing and during the process itself.

8.2 Processing Limitation:

Medical Forum Theatre will ensure that personal information under its control is processed:

- in a fair, lawful and non-excessive manner; and
- only with the informed consent of the data subject; and
- only for a specifically defined purpose; and
- the purpose for processing is adequate, relevant and not excessive.

Medical Forum Theatre will inform the data subject of the reasons for collecting his/her or its personal information and obtain written consent to processing personal information.

Alternatively, where services or transactions are concluded over the telephone or electronic video feed, Medical Forum Theatre will maintain a voice recording of the stated purpose for collecting the personal information followed by the data subject's subsequent consent.

Medical Forum Theatre will under no circumstances distribute or share personal information between separate legal entities, associated Medical Forum Theatre (such as subsidiary companies) or with any individuals that are not directly involved with facilitating the purpose for which the information was originally collected.

Where applicable, the data subject must be informed of the possibility that their personal information will be shared with other aspects of Medical Forum Theatre's business and be provided with the reasons for doing so.

8.3 Purpose Specification:

All of Medical Forum Theatre's business units and operations must be informed by the principle of transparency.

Medical Forum Theatre will process personal information only for specific, explicitly defined and legitimate reasons. Medical Forum Theatre will inform data subjects of these reasons prior to collecting or recording the data subject's personal information.

Records of personal information will not be retained longer than is necessary for achieving the purpose for which the information was collected or subsequently processed.

8.4 Further Processing:

Personal information will not be processed for a secondary purpose unless that processing is compatible with the original purpose.

Therefore, where Medical Forum Theatre seeks to process personal information, it holds for a purpose other than the original purpose for which it was originally collected, and where this secondary purpose is not compatible with the original purpose, Medical Forum Theatre will first obtain additional consent from the data subject.

8.5 Information Quality:

Medical Forum Theatre will take reasonable practical steps to ensure that all personal information collected is complete, accurate, not misleading and updating accordingly.

The more important it is that the personal information be accurate, the greater effort Medical Forum Theatre will put into ensuring its accuracy.

Where personal information is collected or received from third parties, Medical Forum Theatre will take reasonable steps to confirm that the information is correct by verifying the accuracy of the information directly with the data subject or by way of independent sources.

Medical Forum Theatre's suppliers, insurers, and other third-party service providers will be required to sign a service level agreement guaranteeing their commitment to the Protection of Personal Information; this is however an ongoing process that will be evaluated as needed.

8.6 Open Communication:

Medical Forum Theatre will take reasonable steps to ensure that data subjects are notified (are at all times aware) that their personal information is being collected including the purpose for which it is being collected and processed.

Medical Forum Theatre will ensure that it establishes and maintains a contact us facility, for instance via its website or through an electronic helpdesk, for data subjects who want to:

- enquire whether Medical Forum Theatre holds related personal information, or
- request access to related personal information, or
- request Medical Forum Theatre to update and correct related personal information, or
- make a complaint concerning the processing of personal information.

8.7 Security Safeguards:

Medical Forum Theatre will manage the security of its filing system to ensure that personal information is adequately protected.

Security controls will be implemented in order to minimise the risk of loss, unauthorised access, disclosure, interference, modification or destruction.

Security measures also need to be applied in a context sensitive manner. The more sensitive the personal information, the greater the security required.

Medical Forum Theatre will continuously review its security controls which will include regular testing of protocols and measures in place to combat cyber-attacks on Medical Forum Theatre's IT network.

Medical Forum Theatre will ensure that all paper and electronic records comprising personal information are securely stored and made accessible only to authorised individuals.

All electronic files or data are backed up by Medical Forum Theatre's Information Technology and their IT providers who are also responsible for system security to protect against third party access and physical threats.

All new employees will be required to sign employment contracts containing contractual terms for the use and storage of employee information. Confidentiality clauses will also be included to reduce the risk of unauthorised disclosures of personal information for which Medical Forum Theatre is responsible.

All existing employees will, after the required consultation process has been followed, be required to sign an addendum to their employment containing the relevant consent and confidentiality clauses.

Medical Forum Theatre's operators and third-party service providers will be required to enter into service level agreements with Medical Forum Theatre where both parties pledge their commitment to POPIA and the lawful processing of any personal information pursuant to the agreement.

8.8 Data Subject Participation:

A data subject may request the correction or deletion of his, her or its personal information held by Medical Forum Theatre.

Medical Forum Theatre will ensure that it provides a process for data subjects who want to request the correction or deletion of their personal information.

Where applicable, Medical Forum Theatre will include a link to unsubscribe from any of its electronic newsletters or related marketing activities.

9. INFORMATION OFFICERS:

Medical Forum Theatre will appoint an Information Officer and a Deputy Information Officer to assist the Information Officer.

Medical Forum Theatre's Information Officer is responsible for ensuring compliance with POPIA.

Once appointed, Medical Forum Theatre will register the Information Officer and the Deputy Information Officer with the Information Regulator established under POPIA prior to performing his or her duties.

10. SPECIFIC DUTIES AND RESPONSIBILITIES:

10.1 Top Management:

The Top Management is responsible for ensuring that:

- Medical Forum Theatre appoints an Information Officer and a Deputy Information Officer.
- All persons responsible for the processing of personal information on behalf of Medical Forum Theatre:
 - Are appropriately trained and supervised to do so.
 - Understand that they are contractually obligated to protect the personal information that Medical Forum Theatre come into contact with, and are aware that a wilful or negligent breach of this policy's processes and procedures may lead to disciplinary action being instituted against them.
- Data subjects who want to make enquiries about their personal information are made aware of the procedure that needs to be followed should they wish to do so.
- The scheduling of a periodic POPI Audit in order to accurately assess and review the ways in which Medical Forum Theatre collects, hold, uses, shares, discloses, destroys and process personal information.

10.2 Information Officer:

Medical Forum Theatre's Information Officer is responsible for:

- Taking steps to ensure Medical Forum Theatre's reasonable compliance with the provision of POPIA.
- Keeping Top Management updated about Medical Forum Theatre's information protection responsibilities under POPIA.
 - In the case of a security breach, the Information Officer must inform and advise Top Management of their obligations pursuant to POPIA.
- Continually analysing privacy regulations and aligning them with Medical Forum Theatre's personal information processing procedures. This will include Medical Forum Theatre information protection procedures and related policies.
- Ensuring POPI Audits are scheduled and conducted on a regular basis.
- Ensuring that Medical Forum Theatre makes it convenient for data subjects who want to update their personal information or submit POPI related complaints to Medical Forum Theatre.
- Approving any contracts entered into with operators, employees and other third parties which may have an impact on the personal information held by Medical Forum Theatre.
 - This includes overseeing the amendments of Medical Forum Theatre's employment contracts and other service level agreements.
- Encouraging compliance with the conditions required for the lawful processing of personal information.

- Ensuring that employees and other persons acting on behalf of Medical Forum Theatre are fully aware of the risks associated with processing of personal information and that they remain informed about Medical Forum Theatre security controls.
- Organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of Medical Forum Theatre.
- Addressing employee's POPIA related questions.
- Addressing all POPIA related requests and complaints made by Medical Forum Theatre's data subjects.
- 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.

The Deputy Information Officer will assist the Information Officer in performing his or her duties.

10.3 IT Manager (or service provider)

Medical Forum Theatre IT Manager (or service provider) is responsible for:

- Ensuring that Medical Forum Theatre's IT infrastructure, filing systems and other devices used for processing personal information meet acceptable security standards.
- Ensuring that all electronically held personal information is kept only on designated drives and servers and uploaded only to an approved cloud computing services.
- Ensuring that servers containing personal information are sited in a secure location, away from the general office space.
- Ensuring that all electronically stored personal information is backed-up and tested on a regular basis.
- Ensuring that back-ups containing personal information are protected from unauthorised access, accidental deletion and malicious shacking attempts.
- Ensuring that personal information being transferred electronically is encrypted.
- Ensuring that all servers and computers containing personal information are protected by a firewall and the latest security software.
- Performing regular IT audits to ensure that the security of Medical Forum Theatre's hardware and software are functioning properly.
- Performing a proper due diligence review prior to contracting with operators or any other third-party service providers to process personal information on Medical Forum Theatre's behalf.

10.4 Marketing and Communication Manager:

Medical Forum Theatre's Marketing and Communication Manager is responsible for:

- Approving and maintaining the protection of personal information statements and disclaimers that are displayed on Medical Forum Theatre's website, including those attached to communications such as e-mails and electronic newsletters.
- Addressing any personal information protection queries from journalists or media outlets such as newspapers.
- Where necessary, working with persons acting on behalf of Medical Forum Theatre to ensure that any outsourced marketing initiatives comply with POPIA.

10.5 Employees and other Persons acting on behalf of Medical Forum Theatre :

Employees and other persons acting on behalf of Medical Forum Theatre will, during the course and the performance of their services, gain access to and become acquainted with the personal information of certain patients, suppliers and other employees.

Employees and other persons acting on behalf of Medical Forum Theatre are required to treat personal information as a confidential business asset and to respect the privacy of data subjects.

Employees and other persons acting on behalf of Medical Forum Theatre may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within Medical Forum Theatre or externally, any personal information, unless such information is already publicly known or the disclosure is necessary in order for the employee or person to perform his or her duties.

Employees and other persons acting on behalf of Medical Forum Theatre must request assistance from their line manager or the Information Officer if they are unsure about any aspect related to the protection of a data subject's personal information.

Employees and other persons acting on behalf of Medical Forum Theatre will only process information where:

- The data subject or a competent person where the data subject is a child, consents to the processing;
- The processing is necessary to carry out actions for the conclusion or performance of contracts to which the data subject is a party; or
- The processing complies with an obligation imposed by law on the responsible party;
or
- The processing protects a legitimate interest of the data subject; or
- The processing is necessary for pursuing the legitimate interest of Medical Forum Theatre or of a third party to whom the information is supplied.

Furthermore, personal information will only be processed where the data subject:

- Clearly understand why and for what purpose his, her or its personal information is being collected; and
- Has granted Medical Forum Theatre with explicit written recorded consent to process his, her or its personal information.
- Employees and other persons acting on behalf of Medical Forum Theatre will consequently, prior to processing any personal information obtain a specific and informed expression of will from the data subject, in terms of which permission is given for processing of personal information.
- Informed consent is therefore when the data subject clearly understands for what purpose his, her or its personal information is needed and who it will be shared with.

Consent to process a data subject's personal information will be obtained directly from the data subject, except where:

- The personal information has been made public; or
- Where valid consent has been given to a third party; or
- The information is necessary for effective law enforcement

Employees and other persons acting on behalf of Medical Forum Theatre will under no circumstances:

- Process or have access to personal information where such processing or access is not a requirement to perform their respective work-related tasks or duties.
- Save copies of personal information directly to their own private computers, laptops or other mobile devices like tablets or smart phones. All personal information must be accessed and updated from Medical Forum Theatre's central database or a dedicated server.
- Share personal information outside of South Africa without the express permission from the Information Officer.

Employees and other persons acting on behalf of Medical Forum Theatre are responsible for:

- Keeping all personal information that they come into contact with secure, by taking sensible precautions and following the guidelines outlined within this policy.
- Ensuring that personal information is held in as few places as is necessary. No unnecessary additional records, filing systems and data sets should therefore be created.
- Ensuring that personal information is encrypted prior to sending or sharing the information electronically.
 - The IT Manager (or service provider) will assist employees and where required, other persons acting on behalf of Medical Forum Theatre, with the sending or sharing of personal information to or with authorised external persons.
- Ensuring that all computers, laptops and devices such as tablets, flash drives and smartphones that store personal information are password protected and never be left unattended. Passwords must be changed regularly and may not be shared with unauthorised persons.

- Ensure that their computer screens and other devices are switched off or locked when not in use or when away from their desk.
- Ensuring that where personal information is stored on removable storage medias such as external drives, CD's or DVD's that these are kept locked away securely when not being used.
- Ensure that where personal information is stored on paper, that such hard copy records are kept in a secure place where unauthorised people can't access it, for instance, in a locked drawer of a filing cabinet.
- Ensuring that where personal information has been printed out that the paper printouts are not left unattended where unauthorised individuals could see or copy them.
- Taking reasonable steps to ensure that the personal information is kept accurate and up to date.
 - e.g., confirming a data subject's contact details when the patient phones or communicates via e-mail.
 - Where a data subject's information is found to be out of date, the responsible party should update same.
- Taking reasonable steps to ensure that personal information is stored only for as long as it is needed or required in terms of the purpose for which it was originally collected.
 - Where personal information is no longer required, authorisation must first be obtained from the Information Officer to delete or dispose of the personal information in the appropriate manner.
- Undergoing POPI Awareness training from time to time.

11. POPI AUDIT:

The Information Officer will schedule periodic POPI Audits.

The purpose of a POPI Audit is to:

- Identify the processes used to collect, record, store, disseminate and destroy personal information.
- Determine the flow of personal information throughout Medical Forum Theatre.
- Redefine the purpose for gathering and processing personal information.
- Ensuring that the processing parameters are still adequately limited.
- Ensure that new data subjects are made aware of the processing of their personal information.
- Re-establish the rationale for any further processing where information is received via third party.
- Verify the quality and security of personal information.
- Monitor the extend of the compliance with POPIA and this policy.
- Monitor the effectiveness of internal controls established to manage Medical Forum Theatre's POPIA related compliance risks.

In performing the POPI Audit, Information Officers will liaise with line managers in order to identify areas within Medical Forum Theatre's operation that are most vulnerable or susceptible to the unlawful processing of personal information.

Information Officers will be permitted direct access to and have demonstrable support from line managers and Medical Forum Theatre's Top Management in performing their duties.

12. REQUEST TO ACCESS PERSONAL INFORMATION PROCEDURE:

Data subjects have the right:

- Request what personal information Medical Forum Theatre holds about them and why;
- Request access to their personal information; and
- Be informed how to keep their personal information up to date.

All requests will be processed and considered against Medical Forum Theatre's PAIA Manual.

13. POPI COMPLAINTS PROCEDURE:

Data subjects have the right to complain in instances where any of their rights under POPIA have been infringed upon.

Medical Forum Theatre takes all complaints very seriously and will address all POPI related complaints in accordance with the following procedure:

- POPI complaints must be submitted to Medical Forum Theatre 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 a person other than the Information Officer, that person will ensure that the full details of the complaint reach the Information Officer within 1 (one) working day.
- The Information Officer will provide the complainant with a written acknowledgement of receipt of the complaint within 2 (two) working days.
- The Information Officer will carefully consider the complaint and address the complainant's concern 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 POPIA.
- 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 Medical Forum Theatre's data subjects.
- 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 Medical Forum Theatre's Senior Management where after the affected data subjects and the Information Regulator will be informed of this breach.
- The Information Officer will revert to the complainant with a proposed solution with the option of escalating the complaint to Medical Forum Theatre Top Management within 7 (seven) days of receipt of the complaint. In all instances, Medical Forum Theatre will provide

reasons for any decisions taken and communicate any anticipated deviation from the specified timelines.

- The Information Officer's response to the data subject may comprise any of the following:
 - A suggested remedy for the complaint,
 - A dismissal of the complaint and the reasons as to why it was dismissed; or
 - An apology (if applicable) and any disciplinary action that has been taken against any employees involved.
- 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.
- 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 related complaints.

14. DISCIPLINARY ACTION:

Where a POPI complaint or a POPI infringement investigation has been finalised, Medical Forum Theatre may recommend any appropriate administrative, legal and/or advisory action to be taken against any employee reasonably suspected of being implicated in any non-compliant activity outlined within this policy.

In case of ignorance or minor negligence, Medical Forum Theatre will undertake to provide further awareness training to the employee.

Any gross negligence or the wilful mismanagement of personal information, will be considered a serious form of misconduct for which Medical Forum Theatre may summarily dismiss the employee. Disciplinary procedures will commence where there is sufficient evidence to support an employee's gross negligence.

15. RETENTION AND RESTRICTION OF DOCUMENTS:

Records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless –

- a) The retention of a record is required or authorised by law;
- b) Medical Forum Theatre reasonably requires a record for lawful purposes related to its functions or activities;
- c) Retention of a record is required by a contract between the parties thereto; or
- d) The data subject or a competent person where the data subject is a child has consented to the retention of a record.

Information collected or processed initially for the purposes of historical, statistical or research value, may be retained for a period longer than contemplated, provided Medical Forum Theatre has appropriate measures in place to safeguard these records against uses other than what they were intended for initially.

Medical Forum Theatre will destroy or delete a record of personal information or de-identify it as soon as reasonably practical after Medical Forum Theatre is no longer authorised to retain a record.

The de-identifying or deletion of a record of personal information must be done in a manner that prevents its reconstruction in an intelligible/understandable form.

In the event that Medical Forum Theatre uses a record of personal information of a data subject to make a decision about the data subject, it must –

- Retain the record for such period as may be required or prescribed by law or a code of conduct; or
- If there is no law or code of conduct prescribing a retention period, retain the record for a period which will afford the data subject a reasonable opportunity, taking all considerations relating to the use of the personal information into account, to request access to the record.

Medical Forum Theatre will restrict the processing of personal information if –

- Its accuracy is contested by the data subject, for a period enabling Medical Forum Theatre to verify the accuracy of the information;
- Medical Forum Theatre no longer needs the personal information for achieving the purpose for which it was collected or subsequently processed, but it has to be maintained for purposes of proof;
- The processing is unlawful and the data subject opposes its destruction or deletion and requests the restriction of its use instead; or
- The data subject requests to transmit the personal data into another automated processing system.

Personal information that has been restricted may only be processed for purposes of proof, or with the data subject's consent, or with the consent of a competent person where the data subject is a child, or for the protection of the rights of another natural or legal person or if such processing is in the public interest.

Where personal information is restricted, Medical Forum Theatre will inform the data subject before lifting the restriction.

16. SECURITY COMPROMISES:

Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, Medical Forum Theatre will notify –

- a) The Information Regulator; and
- b) The data subject, unless the identity of such data subject cannot be established.

The notification of a breach will 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 Medical Forum Theatre's Information System.

Medical Forum Theatre will 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.

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

- Posted to the data subject's last known physical or postal address; or
- Sent by e-mail to the data subject's last known e-mail address; or
- Placed in a prominent position on the website of Medical Forum Theatre ; or
- Published in the news media.

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

- A description of the possible consequences of the security compromise;
- A description of the measures that Medical Forum Theatre intends to take or has taken to address the security compromise

17. POINT OF CONTACT:

The point of contact for requests, disclosures, questions, complaints and any other inquiries relating to the handling, collection, processing or re-identifying of personal information shall be directed to the Information Officer or Deputy Information Officer(s) as referred to in the Information Officer Policy.

18. REVIEW OF POLICY:

The policy will be reviewed on an annual basis to address any changes in the technical domain, or applicable legislation.

In the event of any critical interim developments regarding the above, immediate revision and adaption will be implemented as soon as reasonably possible and the revised documentation will be circulated and explained to all relevant parties through Medical Forum's Theatre's awareness programs and/or information sessions.