PROTECTION OF PERSONAL INFORMATION (POPI)

1. BACKGROUND

According to the South African Constitution, everyone has the right to privacy but at the same time the right to access any information that is held by another person and that is required for the exercise or protection of any rights.

The Promotion of Access to Information Act **(PAIA)** gives effect to the ***right to access*** of information.

The Protection of Personal Information Act **(POPI)** gives effect to the ***right to privacy***. The POPI Act regulates the processing, collection, storage and disclosure of confidential information with justifiable limitations.

There is an inter-relationship between PAIA and POPI.

The existing healthcare legislation in South Africa provides for protection of personal health information in the following ways:

1. **Confidentiality**

   All personal health information of persons treated in public or private health institutions (health users) or held by medical schemes and managed health care (MHC) organizations is confidential.

2. **Access to Health records**

   A healthcare provider (HCP) may access a person's health records for purposes of treatment provided they have consent from the health user.

   De-identified health information may be accessed and used by a HCP for study, teaching or research without consent.

   A medical scheme is entitled to, subject to certain legislative provisions, to access any treatment record held by a MHC organization or HCP if the medical scheme and the organization or provider concluded a MHC agreement.

Access to records of personal health information by statutory or regulatory bodies is permissible where it is deemed necessary in the interests of justice or for the safety of other patients.

3. **Consent to disclosure**

   The National Health Act, 2003 permits the disclosure of personal health information with the informed consent of the patient. Depending on the nature of the institution the requirements for consent differ.

The aim of the POPI Act is to give effect to the constitutional right to privacy by safeguarding **personal information** of individuals processed by public and private bodies.

An Information Regulator has been appointed to monitor and enforce compliance to this legislation. It will also receive and investigate complaints of violations of POPI and issue codes of conduct for specific sectors.

Giving consent to treatment does not give consent to process or disclose personal information.

2. PROCESSING PERSONAL INFORMATION

Processing can be automatic or non-automatic.

This covers aspects such as:

- Collection
- Receipt
- Recording
- Storage
- Updating
- Use
- Dissemination
- Merging
- Destruction

3. PERSONAL INFORMATION

Personal information is any information relating to an identifiable, living, natural person or existing juristic person.

Personal information covers the following:

- Age, gender, physical or mental health, well-being, disability
- Medical/financial history
- ID number, e-mail, physical address, telephone numbers
- Biometric information e.g. DNA, fingerprint, blood type
- Personal opinions, views, preferences of person
- Correspondence of private or confidential nature
- Views or opinions of another individual about a person
- Name of person. This also depends on additional information that is combined with the name

4. APPLICATION OF THE POPI ACT

POPI is applicable to:

- Medical schemes
- Medical scheme administrators
- Managed health care organizations
- Brokers
- Service providers
- Pharmaceutical companies
- Device companies

It is applicable to automated as well as non-automated systems used to process personal information. Filing systems are referred to as non-automated systems.

POPI is not applicable to:

- Processing of de-identified information that cannot be re-identified (truly anonymous)
- Exemptions granted by the Regulator
- Journalistic purposes subject to conditions

5. THE ROLE PLAYERS

The role players are:

1. The Data Subject (DS)

   This is the person to whom the personal information relates.

2. The Responsible Party (RP)

   This is the public or private body or any other person, alone or in conjunction with others that determines the purpose of and the means for processing personal information.

3. The Operator

   The operator is the person who processes the information or the responsible party in terms of a contract or mandate without becoming under the direct authority of that party.

There might be areas where the above mentioned role players overlap.

6. AUTHORITY TO PROCESS

The types of personal information are divided into the following three parts:

6.1 Other Personal Information

6.2 Special Personal Information

6.3 Personal Information of Children

6.1 Other Personal Information

Specific Authorization for Health Information processed by medical professionals, health care institutions or facilities (section 32) states that such professionals / institutions may process personal information if necessary to provide proper treatment and care or for administrative reasons.

6.2 Special Personal Information

Special personal information covers aspects such as:

- Criminal behavior. Information relating to this may only be collected lawfully after special authorization from the Regulator and with the consent of the person.
- Biometric information. Information relating to this may only be collected lawfully after special authorization from the Regulator and with the consent of the person.
- Health/Sex life
- Religious/Philosophical beliefs

- Trade Union membership
- Political Persuasion
- Race/Ethnic origin. Processing Information relating to race or ethnic origin (section 29) falls under Special Authorization and must be consented to. It must be essential for a specific purpose and comply with laws and regulations.

Processing of Special Personal Information is prohibited unless:

- Authorization is granted by section 27-33
- Regulator approved
- Covered by general authorization during consent
- Special authorization per category of Special PI

Special Authorization is granted to insurance companies, medical schemes, administrators and managed care organizations **only if the information relates** to the processing of inherited characteristics of serious medical interest / historical research or statistical activity.

- Assessment of insured risk must be without objection from the insured.
- Performance of Medical Scheme / Insurance Agreement

  Medical Scheme agreement should cover aspects of Medical Schemes Act, Regulations, Rules and any special arrangement legally agreed between the member and the scheme.
- Enforcement of Contractual Rights and Obligations

Special Authorization should only be obtained if it is necessary in order to provide effective care. Good reason(s) must be present for obtaining this information and such information should be relevant to the situation and justifiable. (e.g. Religion)

6.3 Personal Information of Children (excluding special personal information)

It is important to identify children accurately. A child is a person < 18 years who is not legally competent to take an action / decision regarding him/herself without assistance of a competent person. This results in some application difficulties. The Children's Act refers to the age as 12 years subject to certain conditions and in some cases even younger than 12 years. The choice of termination of pregnancy has no specified age.

In all cases, consent must be acquired from a competent person.
Consent should also cover aspects relating to treatment, information as well as account rendering.

7. THE REGULATOR

Section 37 stipulates when the Regulator **may** allow/approve processing while section 57 – 59 stipulates when the Regulator **must** allow/approve processing.

The Regulator **may** allow/approve processing when the information is in the public interest and the clear benefit of such processing outweighs interference with privacy to substantial degree.

Public interest can be the following:

1. State security
2. Prevention, detection and prosecution of offences
3. Important economic or financial interests of a public body
4. Fostering compliance with legal provisions established in interests referred to in 2 and 3
5. Historical, statistical or research activity
6. Special importance of interest in freedom of expression

The Regulator **must** allow/approve processing of personal information if:

1. Unique identifiers are used for a different purpose and can be linked to information processed by other responsible persons.
2. Information relates to criminal behavior
3. Information is disclosed during credit reporting
4. Special requirements apply when information is transferred to 3rd parties in foreign countries (section 72)
5. Other which may be determined by the Regulator

8. DEALING WITH THE AUTHORITY TO PROCESS PERSONAL INFORMATION

1. The Responsible Party (RP) must have the authority to process in each instance.
2. The different categories of Personal Information (PI) must be identified:

- Health information
- Race
- Biometric information
- Information of children
- Other information – contact details, age, gender etc.
- Processing information could involve a combination of the different categories of PI

3. How is the PI used?
    - Risk assessment
    - Payment of benefits
    - Utilization of benefits
    - Disease management
    - Statutory reporting
    - Ex Gratia decisions
    - Credit reporting
    - Trend analysis
    - Patient care
    - Medical Scheme claims
    - Insurance reports
    - Patient identification

Consent must be voluntary, specific and an informed expression of will in terms of which permission is given for the processing of PI.
Always determine WHAT type of information is involved and WHAT the ground to justify the processing of PI is.

9. To continue

9. CONDITIONS FOR LAWFUL PROCESSING OF PI

1. Accountability

   The Responsible Party must ensure compliance with conditions for lawful processing of PI.

2. Processing limitation

   Processing must be lawful, in a reasonable manner and not infringe on privacy. Information must be adequate, relevant and not excessive for the purpose.

3. Purpose specification

   The RP may only collect PI for specific, explicitly defined and lawful purpose related to the function / activity of the RP.

4. Further processing limitation

   Further retention of documents, therefore retaining PI must be compatible with the purpose for which it is collected.

5. Information Quality

   The RP must take reasonable practical steps to ensure that all PI is complete, accurate, not misleading and updated.

6. Openness

   The RP must maintain information prescribed in respect of all processing operations under its responsibilities. (Section S14/51 of PAIA-to be amended by POPI)

   Specific reference here to the PAIA Manual.

7. Security Safeguards

   The RP must secure integrity and confidentiality of PI by –

   Appropriate, reasonable technical and organizational measures

   Prevent loss, damage, unauthorized destruction and unlawful access / processing

   Generally accepted and applicable information security practices in industry

   Perform risk assessment

   Implement, maintain and update safeguards against risks

   Verify effective implementation of safeguards

   An operator may only process PI with the knowledge / authorization of the RP and must treat PI as confidential and not disclose it. Exceptions: requirements by law or in the course of proper performance of duties.

   A written contract between the RP and Operator must include that the Operator establishes and maintains security measures. The Operator must notify the RP

immediately where on reasonable grounds the PI of a DS was accessed or acquired by any unauthorized person.

Contracts – 3rd parties including switching companies, and/or administrative staff

Should there be reasonable grounds to suspect that PI was unlawfully accessed or acquired, the RP must notify the Regulator as well as the DS in writing. Such notification must advice the DS to take proactive measures against potential consequences.

8. Data Subject Participation

A DS may, after providing proof of identity, request from the RP -

To confirm whether it holds PI (free of charge)

A record / description of PI (prescribed fee)

To whom PI has been disclosed (prescribed fee)

The RP may refuse info requested on grounds of PAIA –

Protection of privacy of a 3rd party who is a natural person (S63)

Protection of commercial information of 3d party (S64)

Protection of certain confidential information of 3rd party (S65)

Protection of safety of individuals and protection of property (S66)

Protection of records privileged from production in legal proceedings (S67)

Commercial information of private body (68)

Protection of research information of 3rd party /private body (S69)

With reference to Health Records, the RP may refuse to divulge information (PAIA S61) if such disclosure of record may cause serious harm to physical /mental health / wellbeing of relevant person. This may result in counseling or other arrangements as are reasonably practical before, during or after disclosure to limit, avoid or alleviate harm to the relevant person.

Personal Information Policy

Should PI be communicated to DS, the RP must advice the DS of the right to request correction of such PI. The DS may request correction / deletion of information that is

inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully.

The RP must then correct, destroy, delete or provide evidence in support of information. Should the RP not agree to corrections as requested by DS, the RP must attach a note to such information that a correction was requested but not made. Following such a decision, the RP must inform the DS of actions taken. Should any corrections be made to PI, the RP must inform every person to whom this information was disclosed if such PI could have impacted on or might impact on decisions taken i.e. DS.

If the DS contest the accuracy of the PI, processing must be restricted until PI has been verified (S34). In this case, processing must be limited to storage, purpose of proof, consent of DS or competent person, in order to protect the rights of another person or if in the public interest.

10. TRANSBORDER FLOW OF PERSONAL INFORMATION

PI of a DS may only be transferred to a 3rd party in a foreign country if –

- The transfer is to the benefit of the DS
- Not reasonably practical to obtain consent from the DS and if the DS would have likely given consent
- Transfer is necessary for conclusion / performance of a contract concluded in the interest of the DS between the RP and the 3rd party
- Transfer is necessary for performance of contract between DS and RP
- Transfer is carried out with the consent of the DS
- Recipient is subject to law / binding corporate rules or agreement. Such transfers should have an adequate level of protection (principles substantially similar to conditions for lawful processing)

Issues relating to Cloud based – storage and Dropbox

11. DIRECT MARKETING THROUGH UNSOLICITED ELECTRONIC COMMUNICATION (S69)

Processing of PI for direct marketing by means of any form of electronic communication including telephones, fax, SMS or e-mail, is prohibited unless the DS

- Consents to such marketing. A request for consent should only be made once.

or

- If the DS is a customer of the RP where the PI only is processed

If contact details are obtained in the context of the sale of a product or rendering of a service, AND for the purpose of direct marketing of RP's own or similar products or services, AND if the DS has no objection at the time of the collection of his/her PI as well as at each of the marketing occasions.

Relates to the Consumer Protection Act

12. CODE OF CONDUCT UNDER POPI (S60-68)

The Regulator could issue Codes of Conduct applying to class of information, specific bodies, and specific activities or to specific industries or professions.

Such a code would include conditions for processing or obligations that are fundamentally equivalent. It would also prescribe measures to protect legitimate interests of DS to automated decision-making.

The Regulator may also review this code and decide on its expiry.

An Adjudicator will preside over complaints.

Noncompliance to this code will result in a breach of conditions for lawful processing.

13. INFORMATION OFFICERS

In a private body, these could be the head of the body, CEO, COO, NOM etc.

Their responsibilities include –

- Encourage compliance
- Dealing with requests made under the Act
- Working with the Regulator i.e. investigations pertaining to the body.

Information Officers must be registered with the Regulator.

In a public as well as private body, Deputy Information Officers deals with the promotion of access.

Identify Information Officer

14. ENFORCEMENT

Complaints are directed to the Regulator.

The Regulator investigates, issue search warrants and/or refer to other regulatory bodies.

An Enforcement Committee recommends action to be taken.

Fines and/or imprisonment	**Administrative Fines**	**Damages (Civil action in Court)**
Offences e.g. non-compliance With enforcement notice	Offence	DS / Regulator obo DS
Fines	Infringement Notice	Irrespective of intent / Negligence by RP - defenses
Imprisonment: 12months – 10 yrs	Max: R10m	Damages, aggravated damages, interest, legal costs

Appeals may be made through the High Court.

RP might suffer reputational damage.

15. SUGGESTED APPROACH

Step 1	Identify the type of PI processed
Step 2	May you process the PI identified?
Step 3	**YES:** Proceed to Step 4 **NO:** Take steps to be able to process and proceed to Step 4 or Stop processing
Step 4	Does processing comply with Conditions for Lawful Processing of PI?
Step 5	**YES:** Compliant **NO:** Take steps to become compliant
Step 6	Unsolicited electronic marketing Automated decision-making Directories Transborder PI

16. CONSIDERATIONS

- The POPI Act has potentially significant implications
- Analyze the information processed and the purpose(s) of such processing
- Analyze stakeholders and their respective roles
- Determine who are your DS
- Ensure you have authority to process the information
- Ensure that you comply to all the conditions for processing
- Review processes and procedures
- Review agreements and documents
- Information management, including record keeping and policies
- IT considerations, including policies i.e. laptops, iPads, iPhones etc.

- Training of staff
- Study the actual provisions of POPI

Policies: Record Keeping, Storage, Destruction, Computer usage, iPhone and iPad usage, Personal Information

Contracts: 3rd parties, staff

Consent: covers all aspects and correctly obtained

IT Security

Information Officer

Transborder flow – DS from other countries / MA from other countries

The Protection of Information Act can be accessed at:

http://www.justice.gov.za/legislation/acts/2013-004.pdf

Sources:

http://www.justice.gov.za/legislation/acts/2013-004.pdf

IHRM Seminar – Protection of Personal Information Act – Esmé Prins – Van den Berg

Protection of personal health information in South Africa – 10 things to know – Norton Rose Fulbright