INFORMATION REGULATOR (SOUTH AFRICA)

Ensuring protection of your personal information and effective access to information

GOVERNMENT NOTICE

INFORMATION REGULATOR

No. R. 2024

THE PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013- REGULATIONS RELATING TO THE PROCESSING OF DATA SUBJECT'S HEALTH OR SEX LIFE BY CERTAIN RESPONSIBLE PARTIES IN TERMS OF SECTION 112(2)(c) OF THE PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013

I, Adv Pansy Tlakula, Chairperson of the Information Regulator, hereby, under section 112(2)(c) of the Protection of Personal Information Act 4 of 2013, make the Regulations in the Schedule.

Adv Pansy Tlakula
CHAIRPERSON: INFORMATION REGULATOR
Date:

SCHEDULE

Arrangement Of Regulations

CHAPTER 1

DEFINITIONS

1. DEFINITIONS

In these Regulations, any word or expression to which a meaning has been assigned in POPIA has the meaning so assigned and, unless the context otherwise indicates:

"administrative bodies"	for the purposes of these Regulations means any responsible party managing and implementing Regulations, laws, and the reintegration of or support for workers or persons entitled to benefit in connection with sickness policies regarding the processing of the special personal information related to the health or sex life of a data subject.
"benefit"	means, for the purpose of these Regulations, a payout or other form of compensation or reimbursement or medical cover due and payable in terms of an obligation in law, insurance policy, or contract.
"competent person"	has the meaning given or assigned to it under Section 1 of the Act.
"consent"	has the meaning given or assigned to it under Section 1 of the Act.
"employer"	means the employer as defined in section 1 of the Occupational Health and Safety Act 85 of 1993, as amended.

“health information”	means personal information relating to the physical and/or mental health of a data subject, including the provision of healthcare services and/or any testing, treatment, and diagnosis which reveals information regarding his/her illness, disability or injury.
“insurance company”	means a company that provides and sells insurance.
“insurance policy”	means a life insurance policy or a non-life insurance policy as referred to in the Insurance Act No.18 of 2017.
“legitimate interest”	means, for the purpose of these Regulations, any processing of personal information of the data subject that involves a clear benefit to the data subject/s that outweighs, to a substantial degree, any interference with the privacy of the data subject that could result from such processing.
“managed healthcare”	means clinical and financial risk assessment and management of health care, with a view to facilitating appropriateness and cost-effectiveness of relevant health services within the constraints of what is affordable, through the use of rules-based and clinical management-based programmes as referred to in the Regulations of the Medical Schemes Act GNR.1360 of 2002 wef 1 January 2003.
“managed healthcare organisation”	means a person who has contracted with a medical scheme in terms of regulation 15A to provide a managed healthcare service as referred to in the Regulations of the Medical Schemes Act GNR.1360 of 2002 wef 1 January 2003.

"medical scheme"	means any medical scheme registered under section 24(1) of the Medical Schemes Act No. 131 of 1998.
"medical scheme administrator"	means any person who has been accredited by the Council in terms of section 58 of the Medical Schemes Act No. 131 of 1998.
"pension fund"	means a pension fund organisation, as referred to in Section 1 of the Pension Funds Act 24 of 1956.
"sex life information"	means any information concerning a data subject's sex life or sexual orientation, or sex.
"the Act"	means the Protection of Personal Information Act 4 of 2013.

CHAPTER 2

PURPOSE OF THE REGULATIONS

2.1 The primary purpose of these Regulations is to:

2.1.1 Assist responsible parties to implement the Act correctly;

2.1.2 Provide better transparency to data subjects on the manner in which their health and sex life information may be used; and

2.1.3 To provide tools to the Regulator and data subjects to challenge the use of the health and sex life information that exceeds the boundaries of the Regulations.

SCOPE OF APPLICATION

3.1 These Regulations shall apply to the processing of health or sex life information by the following responsible parties and applicable operators:

3.1.1 Insurance Companies;

3.1.2 Medical Schemes;

3.1.3 Medical Scheme Administrators;

3.1.4 Managed Healthcare Organisations;

3.1.5 Administrative Bodies;

3.1.6 Pension Funds;

3.1.7 Employers working for administrative bodies or pension funds;

3.1.8 Institutions working for administrative bodies or pension funds;

3.2. Reference to the responsible party(ies) in these Regulations shall refer to the responsible party(ies) specified in sub-Regulations 3.1.1 to 3.1.8.

CHAPTER 3

PROCESSING OF SPECIAL PERSONAL INFORMATION BY CERTAIN RESPONSIBLE PARTIES

4. Authorisation concerning the processing of data subject's health or sex life information

4.1. A responsible party may, subject to section 27 of the Act, not process personal information concerning -

4.1.1. 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.

4.1.2. A responsible party may therefore, generally not process the health or sex life information of a data subject.

4.2. The prohibition on the processing of personal information as contained in section 26 of the Act, does not apply if the –

4.2.1. Processing is carried out with the consent of a data subject as referred to in section 26 of the Act;

4.2.2. Processing is necessary for the establishment, exercise or defence of a right or an obligation in law;

4.2.3. Processing is necessary to comply with an obligation of international public law;

4.2.4. Processing is for historical, statistical or research purposes;

4.2.5. Information has deliberately been made public by the data subject; or

4.2.6. Provisions of sections 28 to 33 are, as the case may be, complied with.

5. Processing of health or sex life by administrative bodies, pension funds, employers, and institutions working for them

5.1. Administrative bodies, pension funds, employers, or institutions working for them may process a data subject's health or sex life information if such processing is necessary for in terms of section 32(1)(f)(i) and (ii) of the Act for the purpose of:

5.1.1. Complying with the obligation imposed by law on the responsible party;

5.1.2. Pursuing the legitimate interests of the responsible party; or

5.1.3. Protecting a legitimate interest of a data subject.

6. Legitimate interest assessment

6.1. Where the responsible party has confirmed that it is necessary for it to process the health and sex life information of a data subject to implement a law, regulation or collective agreement, and where the responsible party relies on section 11(1)(f) of the Act and the consent of the data subject cannot be obtained, such responsible party must conduct a Legitimate Interest Assessment ("LIA") prior to the implementation of the law, regulation or collective agreement.

6.2. The responsible party or third party mentioned in these regulations who process health or sex life in terms of these regulations for the purpose of protecting the legitimate interests of a data subject or pursuing the legitimate interest of a responsible party must conduct a LIA to identify the legitimate interests and determine whether the identified legitimate interest is appropriate to use as a lawful basis for processing personal information.

6.2.1. The responsible party must conduct the LIA before commencing with the processing of personal information concerning a data subject's health or sex life.

6.2.2. Responsible parties must keep records, in terms of section 14(1) and (2) of the Act, of the LIA conducted as a way of demonstrating compliance with section 8 of the Act.

6.3. For a responsible party or third party to rely on legitimate interest as a basis for lawful processing of health or sex life information concerning a data subject's health or sex life information, the following 3 staged assessments must be conducted:

6.3.1. a purpose test to identify the legitimate interest by setting out the purpose for processing health or sex life information concerning a data subject, as well as the benefits associated with the responsible party processing such information;

6.3.2. a necessity test to determine if the processing of such personal information is necessary to achieve the goal/purpose; and whether there are no less intrusive methods that can be used to achieve the goal/purposes; and

6.3.3. a balance test which requires a responsible party to balance their legitimate interest against the interests and rights of the data subject. They must conduct this test by determining the relationship between the responsible party and the data subject, as well as identify the type of personal information being processed and whether it falls within the ambit of special personal information as envisaged in section 26 of the Act.

7. Authorisation to health or sex life information in the public interest

7.1. The processing of the health or sex life information by the bodies mentioned in section 32(1(b) related to the health of a data subject or competent person, by medical schemes, insurance, etc. in the public interest may be authorised by the Regulator upon application in accordance with section 27(2) of the Act.

8. Appropriate safeguards

8.1. The responsible party that processes health or sex life information shall be responsible for maintaining the confidentiality and integrity of such information in its possession or under its control by taking appropriate, reasonable technical and organisational measures in accordance with section 19(1) of the Act which shall include the following:

8.1.1. The protection against any reasonably anticipated threat to the integrity of the health or sex life information:

8.1.1.1. including loss of the health or sex life information, or

8.1.1.2. any unauthorised use, disclosure, unlawful access to or processing of health or sex life information

8.2. The safeguards to be maintained under sub-Regulation 8.1.1. must include appropriate measures for -

8.2.1. the security and confidentiality of records, which measures must address the risks associated with electronic health or sex life records, and;

8.2.2. the proper disposal of health or sex life records to prevent any reasonably anticipated unauthorised use or disclosure of the health or sex life information or unauthorised access to the health or sex life information following its disposal.

8.3. Any processing of health or sex life information must be done provided that there is an agreement between the responsible party and the data subject.

8.4. The responsible parties mentioned in sections 32(1)(b) and (f) of the Act must have due regard to generally accepted information security practices, procedures, and professional rules and regulations that apply to their industry in relation to the processing of health or sex life information of data subjects which must amongst others include the following:

8.4.1. the adoption and implementation of applicable organisational measures, policies, regulations, guidelines, procedures, and requirements to prevent unlawful access or processing of health or sex life information;

8.4.2. in accordance with section 19(2) of the Act, the responsible party must conduct an information security risk assessment, and the mitigation measures (security safeguards) implementation must be enforced. These measures must be regularly evaluated for effectiveness and updated:

8.4.2.1. in accordance with section 19(3) of the Act, these organisational measures must include having an appropriate governance structure to oversee and ensure the adherence to industry standards and generally accepted information security practices; and

8.4.2.2. the adoption and implementation of adequate technical security policies and procedures, internal safety controls, based on applicable ISO standards as recommended by the Health Practitioners Council of South Africa, to protect electronic health or sex life information from any form of loss, damage, unauthorised destruction, and unlawful access.

9. Transfer of personal information outside the Republic

9.1. The responsible party is prohibited from transferring the health or sex life information of a data subject to a third party in a foreign country unless one or more of the requirements set out in section 72(1) of the Act are met.

9.2. Where the responsible party intends to transfer the health or sex life information of a data subject to a third country or international organisation, the responsible party must notify the data subject concerned about such a request before deciding to transfer the health or sex life information in accordance with section 18(1)(g) and (h) of the Act.

9.3. The responsible party should further indicate the level of protection that will be afforded to the personal information by a third party or international organisation to which the personal information is being transferred in accordance with section 18(1)(g) of the Act.

9.4. It is not necessary for a responsible party who intends to transfer personal information to a third party or international organisation to notify the data subject, provided that the data subject has given consent, or such transfer will be in the legitimate interest of the data subject.

CHAPTER 4

RETENTION OF RECORDS

10. Retention of records

10.1. The health or sex life information record of a data subject must not be retained longer than is necessary for achieving the purpose for which the information was collected unless:

10.1.1. The law prescribes the period for which health or sex life records should be retained;

10.1.2. the responsible party reasonably requires the record for lawful purposes related to its functions or activities;

10.1.3. retention of the record is required by a contract between the parties thereto;

10.1.4. the data subject or competent person consents to the storage of his or her health or sex life information to be kept for the prescribed period; and

10.1.5. the health or sex life information is processed for historical, statistical, or research purposes and the responsible party has established appropriate safeguards against the record being used for any other purposes.

CHAPTER 5

DESTRUCTION, DELETION, OR DE-IDENTIFICATION OF HEALTH OR SEX LIFE INFORMATION

11. A responsible party must destroy or delete a record relating to health or sex life information or de-identify it as soon as reasonably practicable after the responsible party is no longer authorised to retain the record in terms of section 14(1) and (2) of the Act. The destruction or deletion of a record of health or sex life information must be done in a manner that prevents its reconstruction in an intelligible form.