WERKSMANS ATTORNEYS

HEALTHCARE & LIFE SCIENCES

The legal and ethical processing of healthcare information

7 June 2023 *10 min read*

The overall objective of the Protection of Personal Information Act No. 4 of 2013 ("**POPI Act**") is to promote the protection of Personal Information (defined below) processed[1] by public and private bodies. Accordingly, the POPI Act establishes the minimum requirements for the processing of the Personal Information and the consequences that may ensue if there is any non compliance with the minimum requirements. In addition to the POPI Act, the National Health Act No. 61 of 2003 ("**NH Act**"), which provides the framework for the South African healthcare system, also sets out the rights and duties of healthcare providers and patients receiving treatment at healthcare facilities. The rights and duties include the patient's right to confidentiality and a corresponding obligation on healthcare providers and facilities to protect the health records of such patients.[2]

The POPI Act and the NH Act, in so far as it relates to the processing of Healthcare Information (defined below), must be considered together with the Health Professions Council of South Africa ("**HPCSA**") Guidelines on Confidentiality: Protecting and Providing Information ("**Guidelines**"),[3] to ensure that Healthcare Information is processed and managed in accordance with the POPI Act (if applicable), the NH Act and the Guidelines.

PROTECTION OF HEALTHCARE INFORMATION

Section 1 of the POPI Act defines "personal information" as information that relates to an identifiable, living, natural person, and where it is applicable, an existing juristic person, including, but not limited to, *inter alia*, information relating to the physical health and well-being of a natural person ("**Personal Information**"). The Guidelines also provide a definition for "personal information" (specific to healthcare providers). In this regard, "personal information" is defined as the patient information that a healthcare practitioner obtains in their professional capacity, and from which individuals (such as patients) may be identified, and such information would include the relevant healthcare records[4] of a patient ("**Healthcare Information**").

The POPI Act (as set out in section 3) applies to the processing of Personal Information –

- "*that has been entered in a record by, or for a responsible party making use of automated (such as any equipment capable of operating automatically in response to instructions) or non-automated means (such a physical filing system); and*
- *where the responsible party is either domiciled in South Africa or makes use of automated or non automated means in South Africa (provided that the automated or non-automated means is not merely used to forward Personal Information through South Africa).*"[5]

Section 32(1)(a) of the POPI Act, provides an exemption for medical professionals, healthcare institutions and other facilities that process Personal Information related to the health and sex life of a data subject. This exemption is, however, only applicable if the processing of the Personal Information pertaining to the health and sex life of the data subject is required to (i) provide proper treatment and care or (ii) for the administration of the professional practice where the treatment is provided to the data subject – the term "proper treatment" is not defined in the POPI Act. The Personal Information related to the health and sex life of a data subject also falls within the category of "special personal information", which a responsible party may not process without the consent of a data subject.

Despite healthcare providers being exempt from complying with the POPI Act, as far as it relates to the provisions of section 32(1)(a) of the POPI Act, such healthcare providers must comply with Chapter 2 of the NH Act. Section 14 of the NH Act provides that all information[6] relating to a healthcare user is confidential and may only be disclosed (i) after obtaining the written consent of such user, (ii) as a consequence of a court order or (iii) if the non-disclosure may present a serious threat to public safety.

The Guidelines (in addition to the NH Act) apply to all healthcare providers that are registered under the Health Professions Act No. 56 of 1974. The Guidelines, therefore, create a duty on healthcare providers to meet the standards of competence, care and conduct set out by the HPCSA, which includes the duty to protect a patient's Healthcare Information. Healthcare providers must therefore be cognisant of the POPI Act, NH Act and the Guidelines when processing Health Information.

MANAGEMENT OF HEALTHCARE INFORMATION

Both the POPI Act and the Guidelines set out the requirements for the lawful and ethical processing of Personal Information and Healthcare Information. In this regard, the POPI Act requires that a responsible party may only process Personal Information in accordance with section 4, read with Chapter 3 of the POPI Act. A responsible party processes Personal Information in a lawful manner if it, *inter alia*, –

- only processes the Personal Information for the purpose for which it was collected;[7]
- obtains the consent of the data subject to process their Personal Information;[8] and
- does not retain the records of the Personal Information for longer than necessary to achieve the purpose for which the Personal Information was collected.[9]

The Guidelines provide analogous requirements, to the provisions of the POPI Act, in relation to the protection of Healthcare Information. The Guidelines require healthcare providers to, *inter alia*, keep all Healthcare Information confidential, which Healthcare Information may only be processed with the consent of the patient and guard against the improper disclosure of such information.

Notwithstanding the similar requirements, in relation to the protection of Personal Information and Healthcare Information, the Guidelines only apply to healthcare providers registered under the HPCSA. To the extent that the exemption under section 32 of the POPI Act applies, healthcare providers will only be bound by the provisions of the NH Act and the Guidelines. Therefore, healthcare providers must be cognisant of the provisions contained in section 32 of the POPI Act to ensure that their management of Healthcare Information complies with the POPI Act (if applicable), NH Act and the Guidelines.

REQUIREMENTS FOR THE MANAGEMENT OF HEALTHCARE INFORMATION

The Guidelines do not preclude healthcare providers from contracting with a third party, who is not registered under the HPCSA, to provide Healthcare Information (which includes Personal Information) management services.

In terms of section 20 of the POPI Act, an operator or anyone processing personal information on behalf of a responsible party (being the healthcare provider) must (i) process the Personal Information only with the knowledge or authorisation of the responsible party, (ii) treat the Personal Information as confidential and (iii) not disclose the Personal Information, unless required by law or in the proper performance of their duties. In addition, section 21 of the POPI Act also requires that the operator establishes and maintains security measures to protect the Personal Information.

As a result, a healthcare provider may appoint a third party operator to assist with the management of Healthcare Information, however, such an appointment will be subject to the operator complying with not only the provisions of the POPI Act (in so far as the information is Personal Information) and the NH Act and the Guidelines (in so far as the information is Healthcare Information). Third party operators (who are not registered under the HPCSA) will, therefore, not be directly obliged to comply with the provisions of the NH Act and Guidelines, The third party operator, acting on behalf of the healthcare provider (registered with the HPCSA), may thus be indirectly and contractually obliged to comply with the provisions of the NH Act and Guidelines, in so far as it acts on behalf of the healthcare provider.

CONSEQUENCES FOR NON-COMPLIANCE

The consequences for non-compliance with the POPI Act are set out in section 109 of the POPI Act, which also sets out the process by which such non-compliance is regulated. In terms of section 109(2)(c) of the POPI Act, an administrative fine, not exceeding R10 million (as may be amended from time to time) may be imposed due to a responsible party's non compliance with the POPI Act.

Even though the Guidelines are silent on the consequences for any non-compliance with its provisions, the non-compliance by the healthcare provider may result in the HPCSA investigating a claim of unprofessional conduct (for acting unethically) against the healthcare provider in terms of Chapter IV of the Health Professions Act No. 56 of 1974.[10]

CONCLUSION

The processing of Personal Information and Healthcare Information will be subject to the provisions of the POPI Act (to the exclusion of information related to the health and sex life of the patient where the exemption in section 32 of the POPI Act applies), NH Act and the Guidelines. The applicable legislation and Guidelines apply irrespective of whether a healthcare provider is processing such information or contracting with a third party operator to perform Healthcare Information management services on its behalf.

The distinction between healthcare providers and third party operators is, therefore, that there is a direct obligation on healthcare providers to comply with the POPI Act, NH Act and the Guidelines, whilst third party operators (who are not registered with the HPCSA) are only required to comply as a

consequence of the Healthcare Information management services they provide on behalf of healthcare providers. Notwithstanding the distinction, the Personal Information and Healthcare Information of a patient must be adequately safeguarded, as the POPI Act, the NH Act and the Guidelines provide similar protective measures to prevent the unlawful and unethical processing of such information and to reinforce a patient's right to privacy and confidentiality.

POPIA and consent, the biggest misunderstanding?

Footnotes

[1] "**Processed**" means any operation or activity or any set of operations, whether by automatic means, concerning Personal Information, including –

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

("**processing**" and "**process**" have the same meaning).

[2] See section 14 and section 17 of the NH Act.

[3] Guidelines on Confidentiality: Protecting and Providing Information published by the Health Professions Council of South Africa in September 2016.

[4] The Guidelines on the Keeping of Patient Records published by the Health Professions Council of South Africa in September 2016 states that healthcare records include the following documents –

- handwritten contemporaneous notes taken by the healthcare practitioner;
- notes taken by previous healthcare practitioners, attending healthcare or other healthcare practitioners, including a typed patient discharge summary or summaries;
- referral letters to and from other healthcare practitioners;
- laboratory reports and other laboratory evidence such as histology sections, cytology slides and printouts from automated analysers, X-ray films and reports, ECG races, etc.;
- audio-visual records such as photographs, videos, and tape recordings;
- clinical research forms and clinical trial data;
- other forms completed during the health interaction such as insurance forms, disability assessments and documentation of injury on duty; and
- death certificates and autopsy reports.

[5] See section 3, read with section 1 of the POPI Act.

[6] This includes information relating to the healthcare user's health status, treatment or stay in a healthcare facility.

[7] See section 10 of the POPI Act.

[8] See section 11 of the POPI Act.

[9] See section 14 of the POPI Act.

[10] The Health Professions Act No. 56 of 1974 not only establishes the HPCSA but regulates the conduct of healthcare providers who are registered under the Health Professions Act No. 56 of 1974.



Neil Kirby

Head of Healthcare & Life Sciences

View Profile



Janice Geel

Associate

View Profile