1. What is personal information?

POPI Act defines personal information as information relating to an identifiable, living, natural person and where applicable, an identifiable, existing, juristic person like for example an incorporated practice (Inc). Personal information includes general and special information.

Information type	Examples
General personal information	Full name and identifying details like identity number and/or passport number
	Contact details, including but not limited to telephone numbers, email address, fax number, physical and postal address.
	Medical aid number, Tax number
	Employment details including employment number and designation
	Education details including student number, qualifications, education reports, etc.
	Bank account details
Special personal information	Religious or philosophical beliefs
	Race or ethnic origin
	Trade union membership and political persuasion
	Health or sex life or any other biometric information
	Biometric information about the data subject

It is clear from the definition that health practices during their operations process vast quantities of personal information, which makes it imperative that the information is protected. Of importance is that de-identified data or an address without a name is not deemed personal information.

2. POPI Act compliance requirements

a. Information Officer

The first and the most important requirement is for the practice to appoint an information officer and register him or her with the Information Regulator. The information officer will be the accountable person for compliance requirements to both the PAIA and POPI Acts. Practice information officers must be registered with the Information Regulator, best done via the Information Regulator Online Portal - https://www.justice.gov.za/inforeg/portal.html

b. POPI Act impact assessment

The practice needs to assess where current structures and processes relating to the collection, transmission and storage of personal information may expose the business to potential POPIA non-compliance. Where weaknesses and gaps are noted, these should be addressed. High risk and vulnerable areas of the practice can be identified by assessing the following areas -

- From whom the practice obtains personal information. (e.g., patients, research subjects, industry representatives)
- The types of personal information being processed by the practice.(e.g., demographics, clinical examination, special investigation results)
- The processing activities being carried out by the practice or on behalf of the practice.
- Which persons in the practice have access to personal information and the type of personal information they have access to.
- Who makes changes to personal information and in what circumstance.
- Which third parties process personal information on behalf of the practice. (e.g., billing companies)
- To whom and for what purpose the information is generally sent. (e.g., other treating and/or consulting providers, medical aids, brokers and insurers, family members, employers)
- Whether personal information is sent across the borders of the Republic of South Africa to persons in other countries, and if other countries, which.
- or how long the practice keeps records (all records of personal information).
- If any direct marketing (electronic or otherwise) is done by the practice using, for example, contact information of patients.
- Security measures to protect personal information.
- Understanding of POPI Act by employees and identification of training needs.

On completion of the assessment, practitioners should compile a list of areas within the practice that need attention and ensure that these are addressed. This may include introduction of or amendments to consent forms, practice-specific policies and protocols and review of third-party and/or employee contracts, as well as training workshops.

c. Policies and Documents

It is important that the practice has the following documents -

- ***Privacy policy*****:** The policy provides an outline of how the practice will comply with the requirements of the Act. It describes, amongst others, how you collect the information, the type of information collected, why that information is collected, the circumstances under which that information will be shared with others, the security measures that will be implemented to protect the information and how others may obtain access to and correct their information.
- ***PAIA manual*****:** The manual is required to set the legal parameters on how patients and third parties can access information held by the practice. The manual also assists with legal remedies when access to information is denied.
- ***Record keeping policy:*** This document provides a guideline on how documents or records will be retained or destroyed by the practice. It is advisable that this policy document takes into consideration the HPCSA guidelines on patient records and POPI Act requirements.

- ***POPI Act consent form and/or clauses:*** The practice is encouraged to develop or obtain POPI Act consent clauses to be included in the existing patient registration documents. A POPI Act standalone consent form is also recommended.

3. Take-home message

- All healthcare practices, irrespective of their size or type are obliged to comply with the requirements of the POPI Act.
- It is advisable that a POPI Act compliance file that contains documents and/or records that are required to demonstrate POPI Act compliance is compiled for the practice. Other than ensuring a systematic and focused approach towards implementation of POPIA compliance by the practice, it ensures ready availability of required information in case the Information Regulator conducts a POPI Act compliance audit.
- Practices need to maintain a balance between POPI Act requirements and HPCSA guidelines and ensure that there are no contradictions between the two statutory requirements, especially when it comes to patient records/information. In case of a conflict between POPI Act and HPCSA, practitioners are encouraged to seek medicolegal advice.
- For further guidance, access the POPIA checklist here (link).