Prepared in collaboration
with Webber Wentzel

PROTECTION OF PERSONAL INFORMATION ACT, 2013 ("POPIA")

Guidance Note for POPIA Compliance by Institutions and Individual practitioner healthcare providers

What does POPIA do?
POPIA gives effect to the constitutional right to privacy by safeguarding personal information of individuals and where appropriate, juristic persons such as companies or associations (called data subjects) which is processed by public and private persons, including individuals (called responsible parties). The healthcare sector handles some of the most sensitive information such as physical and mental records of patients, x-rays, MRI scans and notes made by doctors during consultations and the medical history of patients.

In addition to the' obligations in handling the personal information of patients under the National Health Act, 2003 and the guidelines issued by the Health Professions Council of South Africa under the Health Professions Act, 1974, POPIA imposes minimum standards on the way personal information is processed and that includes the collection, storage usage , disclosure, and deletion of that information.

This note sets out a practical guideline to assist healthcare providers both in institutional organisations and individual practitioners running single practices comply with these obligations. As a matter of priority, you must designate an internal Information Officer (e.g. legal officer or practice administrator) who must register with the Information Regulator (the enforcement agency responsible for monitoring and enforcing compliance with POPIA). The Information Officer must deal with requests made to the business practice under POPIA and will generally be responsible for the practice's compliance with POPIA.

This guidance note is not an exhaustive list of the obligations under POPIA. It does not constitute legal advice and should not be considered a substitute for legal advice.

What is personal information?
Personal information has a wide meaning and refers to information relating to identifiable, living, natural person or an existing juristic person and includes information relating to race, gender, sex, marital status, national, ethnic or social origin, sexual orientation, age, physical or mental health, medical history, biometric information and contact details of a person. The healthcare sector is an industry that relies heavily on information about individually identifiable persons, their state of health and their financial position.

Personal information relating to children (i.e. persons under the age of 18 years) and special personal information (which includes private information relating to religious beliefs, race, and health or sex life) is deemed sensitive information and therefore subject to more onerous processing obligations.

Consent to processing
Under the relevant healthcare legislation, health services may not be provided to a patient without their informed consent.

In terms of POPIA, a patient must, except in certain circumstances, consent to the processing of their personal information. This is usually at contract entering stage. Consent under POPIA is a voluntary, specific, and informed expression of willingness to give permission to process personal information. Where information is collected for any use that requires consent, you must take steps to ensure that the patient is made aware of your identity or your organisation's identity, what information is being collected, what the information will be used for and who the recipients will be. If you need consent, make sure that it is clearly word and is in plain language.

A clause along the following lines may be included in your already existing consent and/or admission forms:

*"By signing this contract and/or informed consent form, you/*the patient agree(s) to the use of your/*the patient's personal information as required under the Protection of Personal Information Act, 2013. You /*the patient also consent to the sharing of your /*the patient's personal information with third parties such as other medical professionals for purposes of rendering treatment to you /*the patient and with medical schemes for billing purposes".*

When is consent not required?
There are limited circumstances where consent will not be required. Consent is not required:

- where the processing protects a legitimate right of the data subject i.e. the patient
- where it is necessary for the responsible party's legitimate interest, or those of a third party
- For the performance in terms a contract that the data subject is a party to. As a responsible party, a hospital or a doctor will have the right to use the personal information (where consent has been given at contract entering stage) to implement the doctor-patient contract

or the hospital admission contract. Not only is this a fulfilment of a contract to which the patient is generally a party but is also in furtherance of the legitimate interests of both the patient and the medical provider as a responsible party. Healthcare institutions or practices are therefore authorized in terms of the patient-doctor contract or hospital admission contract to access, examine and disclose personal information of patients for the proper treatment and care of the patient or administration of the institution or practice.
- When the law requires the processing, for example for discovery purposes in a pending litigation
- a public body needs to perform a public law duty

Case managers and practice or hospital billing staff do not require the patient's consent to collect and process health information during either case management or medical scheme billing submission. But you still need to be mindful of what you do with the information provided in the healthcare contractual context. For this reason, clinician documents and hospital admission contracts must be carefully worded to delineate the various users of information. You also need to explain some concepts to the patient, or their next of kin who is providing information in circumstances where the patient is a child or has limited contractual capacity.

Can you share personal information with third parties?
You must keep the personal information of patients confidential.

As healthcare practitioners, you are already under a legal and professional duty to maintain the confidentiality of patient health information in terms of the National Health Act and the Health Professions Act read with the guidelines. POPIA continues this requirement but also explains that you can disclose information to third parties such as medical schemes or to anyone within the practice or institution administrators if the disclosure is necessary to perform the contract or for practice administration purposes.

You can also disclose personal information if required by law, for example, where the information is required to be disclosed in terms of the Promotion of Access to Information Act or to a regulator. The safest method however is to ensure that your reports only go to people who need to know.

What measures should be in place to secure the personal information?
The biggest exposure under POPIA is the required security safeguarding of personal information. You must take reasonable measures to prevent the loss or damage to or the unauthorized destruction of personal information that is in their possession. You must ensure that you or any third party who processes personal information on your behalf establish and maintain the security measures required by POPIA. To give effect to the above, you must identify:
- the risks to personal information
- establish and maintain safeguards against risks
- regularly verify effectivity of safeguards
- update safeguards if new risk is identified

A lot of data breaches occur due to hacking but also due to human error, for example, leaving a patient file out in the open and it gets lost. Or a flash stick is misplaced. It is often the human element that places institutions most at risk when it comes to data privacy and protection and you need to ensure that you have secure and modern systems in place to protect the information of your patients and of your employees.

Any third party who processes personal information on your behalf will also need to establish and maintain the security measures required by POPIA. This becomes relevant where medical scheme administrators ask you to collect and provide information concerning members of administered schemes. In that context, the administrator becomes a responsible party and you, an operator. An 'operator' is a person who processes personal information for a responsible party in terms of a contract or a mandate, without coming under direct authority of that person. POPIA requires an operator or anyone processing personal information on behalf of a responsible party to do so with the knowledge or authorization of the responsible party.

Record retention periods
Patient information may not be retained longer than is necessary to fulfil the original purpose for collection except where the patient consents, the retention is required by contract between the parties or where the retention of the records is required by law.

You must destroy or delete or de-identify personal information as soon as reasonably practicable after authorisation to retain the records ends. Deleting information from an IT system is not the same as destroying it. Destroying requires physical deletion such as shredding or burning of the information in hardcopy or de-encrypting or using software to overwrite electronic records.

Penalties and offences
POPIA creates significant civil and criminal law exposure where there are breaches. A civil remedy is provided to the person whose data privacy is breached, whether or not there is intent or negligence on the part of the responsible party. Contraventions of certain provisions of POPIA are a criminal offence, rendering the offender liable to a fine or imprisonment up to 10 years or to both a fine and imprisonment. So, ensuring efficient and working systems to protect the confidentiality of personal information is essential.

Conclusion
Generally, obtaining the patient's consent will overcome any hurdles to the provision of processing personal information during treatment and thereafter. Before drafting consent clauses in your contracts, ask: What information do you hold for personal identifiable patients or employees; Are you asking for consent where you do not need it? Where you do need the consent, is it valid under POPIA?

As institutions or practices providing medical and healthcare, you should already have adequate systems in place to protect personal health information given to you by your patients. But a thorough review of your current systems and security safeguards is necessary.

Your contracts with third parties need to include POPIA compliant clauses including appropriate warranties and indemnities as to compliance by those third parties in so far as confidentiality and security measures is concerned.