POPIA CHECKLIST

Steps	Item	Description	Practical guidance
1.	Appoint an information officer for the practice and register such a person with the information regulator.	By default, the head of the practice or the managing director of the practice will be the information officer if a specific person is not appointed. The information officer has a number of duties, which include: • Encourage compliance by the practice with the conditions for the lawful processing of personal information; • Ensure compliance with the practice with the provisions of POPIA; • Ensure the development, implementation, monitoring and maintenance of a compliance framework; • Ensure that a personal information impact assessment is done to ensure that adequate measures and standards exists in order to comply with the conditions for the lawful processing of personal information; • Ensure that a PAIA manual is developed, monitored, maintained and made available as prescribed in PAIA; • Ensure that internal measures are developed together with adequate systems to process requests for information or access thereto; and • Ensure that internal awareness sessions are conducted regarding the provisions of POPIA and its regulations, codes of conduct or information obtained from the information regulator.	You can register online on the information regulator's website by going to the following link https://www.justice.gov.za/inforeg/portal.html or you can email the information officer a completed registration formregistration.IR@justice.gov.za, but we encourage you to follow the former option.

2.	Review your access to information	You are encouraged to perform an impact assessment of the personal information by identifying high-risk and vulnerable areas of your practice by considering: • The types of personal information being processed by the practice; • the processing activities being carried out by the practice or on behalf of practice; • which persons in the practice have access to personal information and the type of personal information they have access to; • which third parties process personal information on behalf of the practice; • whether personal information is sent across the borders of the Republic of South Africa to persons in other countries. Which countries in general? • To whom and for what purpose is the information generally sent? • if any direct marketing (electronic or otherwise) is done by the practice using, for example, contact information of patients; • if any profiling of any person or entity is done by the practice and how the profiles are used; • from whom the practice obtains personal information (all the sources); • for how long the practice keeps records (all records of personal information); • who makes changes to personal information and in what circumstance.	Keep a copy of your impact assessment in your records. All physical access to information (e.g., patient files) must be secured and accessed by designated staff only. Computer systems to have security controls in place to ensure access only by authorised individuals. Prepare a standard operating procedure document specifying which personal information may be disclosed to patients/third parties and under which circumstances.
3.	Prepare a privacy statement	The privacy statement (a.k.a. "privacy policy") describes how personal information will be handled by your practice. It describes, amongst others, how you collect the information, the type of information collected, why that information is	Obtain a privacy statement (policy) for your practice to use which includes POPIA related clauses. This is to be shared with existing patients and to be made readily available at your practice.

		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.	
4.	Revise and enhance patient documentation	Patient registration documentation should be updated to include relevant clauses from the privacy policy (including consent forms) and only include information which is required at a minimum to process patient information (i.e., relevant, necessary and not excessive). Always keep in mind that whichever system you are utilising for purposes of capturing patient personal information, that system must have the ability to record a patient's consent, their withdrawal of consent, record any objections against the processing of personal information, record to whom personal information of patients are disclosed (i.e., the recipients of personal information), and the ability to make notes on the system where corrections to patients' information are required.	Obtain a consent POPIA clause to include in your existing patient registration documentation or as a stand-alone document. Please note that these clauses should be amended in line with your practice's specific requirements.
5.	Ensure information quality	Only up-to-date and correct personal information can be processed. Accurate information about your patients is important since it can impact your communication with them and their health. Patients can request the correction or deletion of any of their personal information.	Upload a copy of Form 2 (as set out in the regulations published under Government Gazette No 42110 dated 14 December 2018) to your website or made available at your reception for this purpose. Patients should be requested to provide current biographical and contact details, and practices to update their records.
6.	Have a retention policy	You should prepare or update your internal policies and procedures to include a formal policy regarding the period that patient records are retained. Information which is older than the agreed period is to be properly disposed or deleted.	It is important to keep in mind, in line with the HPCSA guidelines, that all patient records (including financial records) of adults who are of sound mind should be retained for a period of at least six years from the date the records became dormant. All patient records (including financial records) of minors should be kept until the age of 21 years, in line with the HPCSA guidelines. All patient records (including financial records) of patients who are not of sound mind (i.e., *non compos mentis*) and should be kept for the lifetime of the patient, in line with the

			HPCSA guidelines.
7.	Accessibility to personal information	All personal information (physical and digital) relating to patients should be accessible and shareable with patients on request. This right of access to information is authorised by the Promotion of Access to Information Act 2 of 2000 (PAIA). Patients who wish to exercise this right must complete the prescribed form and submit it to the information officer or your reception. It is always recommended that requests made for records in terms of PAIA are referred to your Professional Indemnity Provider for guidance and assistance.	Compile a PAIA manual for the practice or update your existing manual. Make it available on your website and available at the reception desk of your practice.
8.	Third party contracts	All contracts with third parties to be reviewed and POPIA clauses to be included, where relevant (i.e., undertakings related to compliance with POPIA and security breaches).	Most service providers will update their agreements to this effect, but we suggest that you ensure that these contracts have undertakings to the effect that: • they shall comply with POPIA; • they shall implement and maintain appropriate and reasonable security measures to safeguard personal information; • they shall safely secure all such personal information when processing; • they shall notify you promptly from the date of obtaining knowledge of any data security breach in respect of such personal information and cooperate with you in making any disclosures to affected parties; • it shall not permit any representative or third-party operator to process such personal information, unless it is in compliance with this agreement; • it shall not disclose such personal information to any third party unless it is necessary in order to carry out their obligations, they have obtained your prior written consent and they remain responsible for any breach.
9.	Security and external	Review your policies and procedures for security mechanisms and external communications, with suitable	Assess the people, processes, and technology in terms of weaknesses that relate to the security of personal

	communications	technology to enable deployment.	information. Identify reasonably foreseeable risks (internal and external) to personal information in the possession or under the control of the practice. Establish and maintain appropriate safeguards against these risks. Verify on a regular basis that the safeguards are effectively implemented. Update the safeguards continually when new risks or deficiencies are identified. Consider measures such as physical security of the offices where information is held, locking of cabinets with physical records, password control to access electronic records, offsite data backups and stringent policies in respect of electronic records storage and dissemination. Always keep in mind that the more sensitive information the more stringent your security mechanisms should be. Electronic information should be secured by firewalls, anti-virus, VPN networks, and password secured access. Accidental access must be reported to the information officer immediately. Notification in writing to the affected patients (i.e., data subjects) and reporting to the information regulator, should the personal information relating to the patient be compromised or should there be a suspicion that the personal information is compromised. All security and access breaches or suspected or potential breaches of personal information must be reported to the information regulator immediately after such breach or potential breach becomes known.
10.	Training	To demonstrate your commitment to the protection of personal information it is important to create a culture of vigilance and awareness by ensuring that your employees, contactors, vendors, committee members and any person who may process personal information for and on your behalf, are trained on an annual basis.	Ensure that training takes place, at least, on an annual basis on your privacy policy. This training should also form part of new employee inductions. Ensure that your employees demonstrate a culture of POPIA awareness by having clean desks without openly displaying personal information of patients, using passwords, and being

		mindful around communicating confidential patient information verbally around other patients, especially in the waiting area. Records of POPIA training should be kept in your POPIA file and personnel records. Employment contracts to also be reviewed and POPIA clauses to be included, where relevant (i.e., undertakings related to compliance with POPIA and security breaches).

Various firms provide POPIA documents and further advice, such as Health Navigator run by attorney Esmé Prins-van der Berg, contactable via esme@healthcarenavigator.co.za.