

POPIA Compliance Checklist for Medical Practices

An eight-point self-audit for South African clinicians. Tick each item you can evidence today.

Patient records are “special personal information” under the Protection of Personal Information Act, which sets the bar for handling them higher than for ordinary data. Work through the eight checks below; anything unticked is your compliance to-do list.

☐ **Information Officer registered with the Information Regulator**

Every practice needs one — in a small practice this is usually the practice owner. Registration is done directly with the Information Regulator.

☐ **PAIA manual and privacy notice published**

Both must be available to patients — on your website if you have one, or on request at the practice.

☐ **Patient data collected for clear, stated purposes only**

Collect what the consultation and its administration require, tell patients why, and use it for nothing else.

☐ **Records encrypted, access-controlled and audit-logged**

Whether paper or digital, records need protection against loss and unauthorised access — encryption, per-user access and an audit trail for digital systems.

☐ **Written operator agreements with every vendor**

Any software vendor or billing bureau that touches patient data processes it on your behalf and needs a written operator agreement.

☐ **A breach-notification plan in place**

Know in advance who assesses an incident, who informs the Information Regulator and affected patients, and how quickly.

☐ **A process for patient access and correction requests**

Patients may ask what you hold about them and have it corrected. Decide how requests are received, verified and answered.

☐ **A retention schedule aligned to HPCSA rules**

Keep records as long as the HPCSA requires, then dispose of them securely — retention and destruction are both part of compliance.

Review cadence: re-run this checklist annually, and whenever you change practice software, add a billing bureau, or take on staff who access patient records.