Think Privacy.

POPIA for your practice.

Tips on how to prepare your practice for **POPIA**.

CompuGroup Medical

Content

Get your POPI Act together.

With the enforcement date of the Protection of Personal Information Act 4 of 2013 (POPI) of 1 July 2021 fast approaching, practices should be reviewing their use of personal information to determine whether it complies with the Act.

This document guides you through the most important aspects of POPIA. It provides you with practical tips on how to apply the guidelines in your practice and shares what opportunities POPIA provides to your practice.

For more information on POPIA visit **www.cgm.com/za-popia2021**

POPIA explained.

The POPI Act came into effect on 1 July 2020, but gave a 12-month grace period for businesses to prepare. Your practice must be aligned by 01 July 2021 with the requirements of POPIA. POPIA concerns both public and private organizations situated within and outside the Republic of South Africa handling the Personal Information of South African citizens. POPIA is South Africa's equivalent of the EU's GDPR.

The purpose of POPIA is to protect people and organisations from harm by protecting their Personal and Special Personal Information.

Types of Personal Information

physical address	gender	pregnancy	education	correspondence	age	date of birth
opinions	health status	e-mail	marital status	language	identity number	employment history
disability	preferences	phone number	biometrics	name	others' opinions of you	

Types of Special Personal Information

health information	sex life	religious beliefs	race	political persuasion
ethnic origin	criminal behaviour	philosophical beliefs	trade union membership	

All Personal Information relating to your Patients' health qualifies as Special Personal Information.

Remember, Personal Information always belongs to the Data Subject. So, for example, the Personal Information in a patient's file belongs to the patient, not to you. You are merely the custodian of that information, with a duty to store the Personal Information securely, to ensure that it is kept up to date, and to be able to provide it to the Data Subject on request.

POPIA sets conditions for when it is lawful for someone to process someone else's personal information and when it is not.

For more information on POPIA visit **www.cgm.com/za-popia2021**

POPIA as an opportunity.

You might perceive POPIA to be a daunting task or an administrative burden. You are not all wrong. It is extra work - but at the same time it is an opportunity to assess your business' best practice and ensure that your own, your practice's, staff's, and patients' Private Information is secure at all times. Here are three reasons why POPIA is an opportunity rather than a threat.

You will figure out what personal patient information you collect and process.

POPIA requires you to be able to justify why you are holding Personal Information in your practice. This is a good opportunity to assess what information you are collecting and processing from your patients as well as from staff, and to review whether the information is actually required.

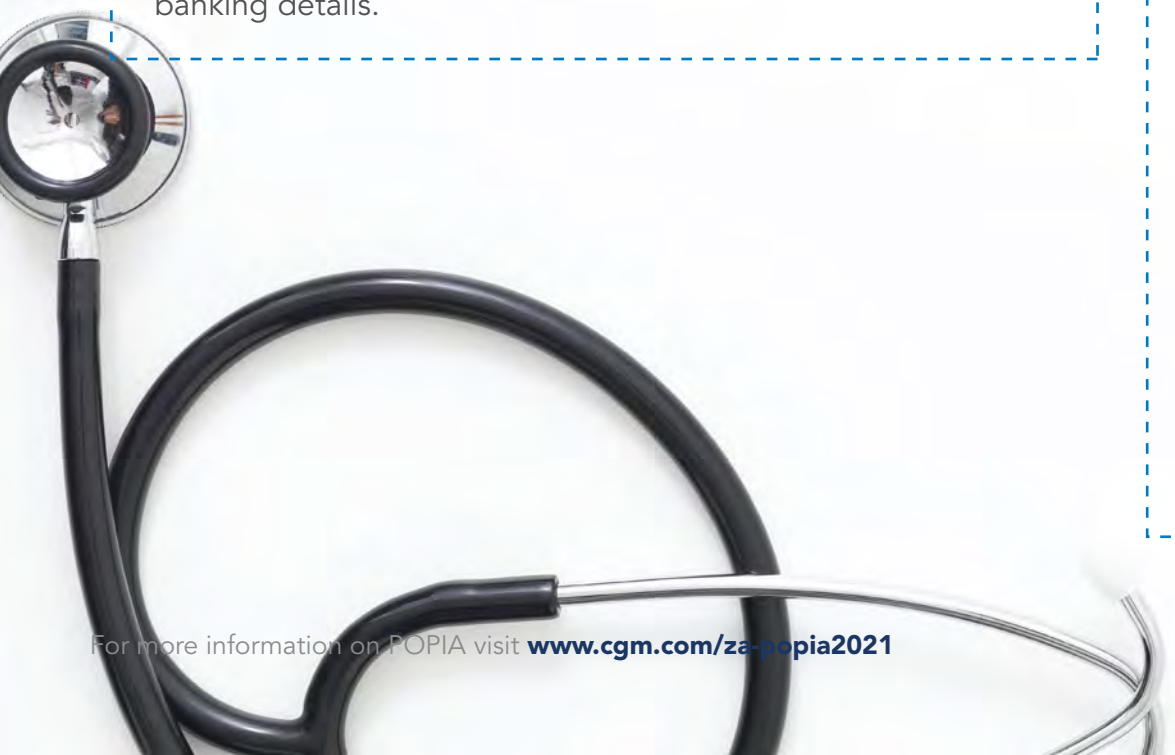
For example, is it necessary for the practice to know whether or not someone is married, or what race they are, or what their profession is? Also, be aware of how you collect the information in the first place. So, if a patient fills out a form in the waiting room and either misses out a question or writes something illegible, calling out to them across a packed waiting room to confirm a phone number or street name constitutes a violation of POPIA.

For more information on POPIA visit **www.cgm.com/za-popia2021**

You will get rid of what you do not need.

POPIA ensures that you do not keep records of Personal Information if there is no reason to do so. If you do not need a record anymore and are not obliged to keep it by law, you should dispose of it in a secure way.

So, for example, when you hire new staff for the practice, the CVs of unsuccessful applicants should not be left to moulder in a drawer or inbox. They should be shredded asap. For that matter, any sheet of paper containing any Personal Information, particularly health information, should be shredded rather than being scrunched up and thrown into a waste paper basket. Criminal gangs pay people to sort through rubbish looking for Personal Information. Currently, health information is more valuable on the black market than banking details.



You will turn data security and privacy into a habit.

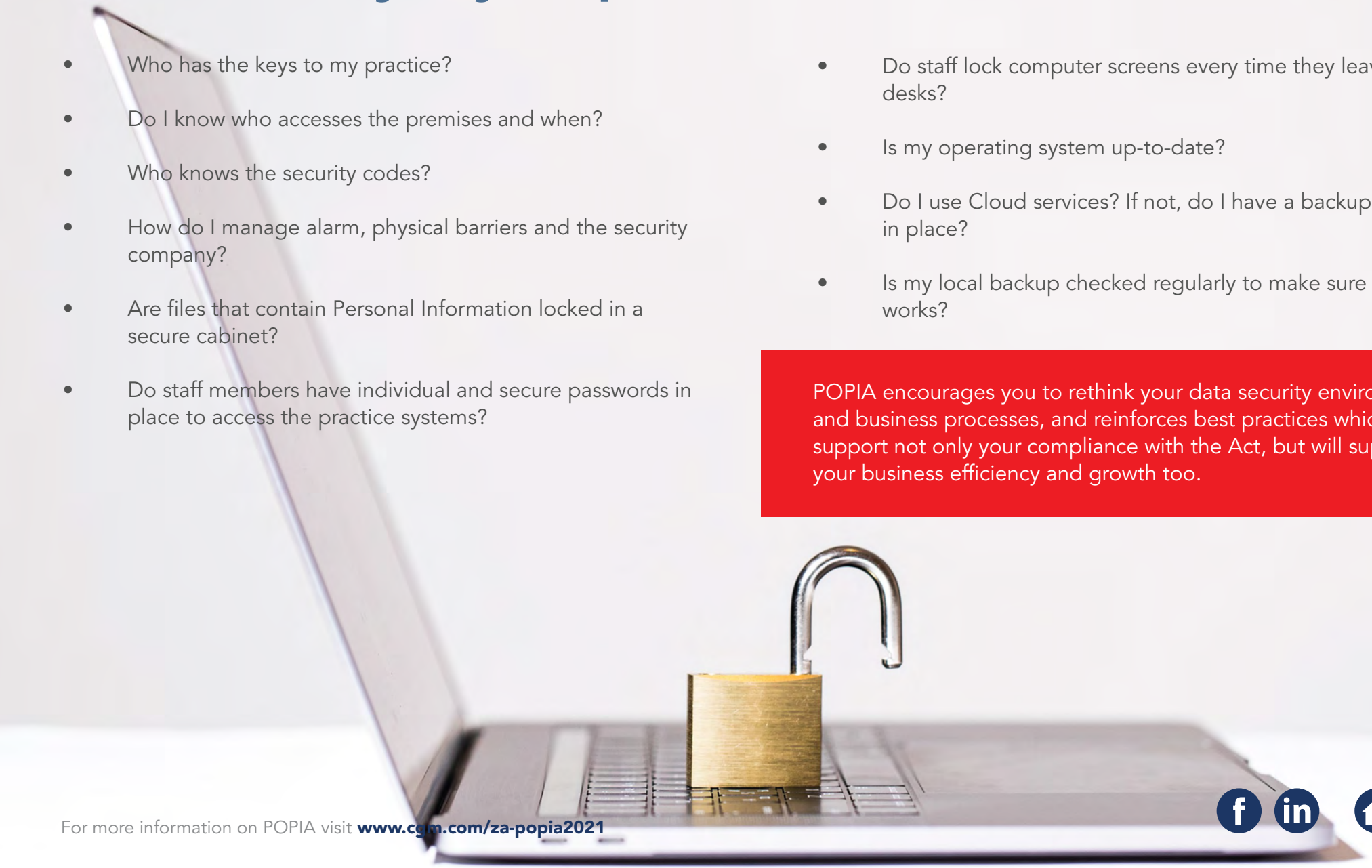
To manage and protect personal information the appropriate data security measures as well as procedures must be put in place and maintained. This concept is not new but was there long before POPIA to prevent loss, theft or damage to personal information. The HPCSA's booklets 4, 5 and 9 already contain many of the POPIA principles as they apply to the healthcare sector regarding protection of patient privacy and obtaining consent.

By going through the process of auditing your practice's physical and electronic security measures, you will come to understand the vulnerabilities, and what measures you need to put in place to secure the Personal Information in your custody.

Questions you need to ask yourself about security in your practice.

- Who has the keys to my practice?
- Do I know who accesses the premises and when?
- Who knows the security codes?
- How do I manage alarm, physical barriers and the security company?
- Are files that contain Personal Information locked in a secure cabinet?
- Do staff members have individual and secure passwords in place to access the practice systems?
- Do staff lock computer screens every time they leave their desks?
- Is my operating system up-to-date?
- Do I use Cloud services? If not, do I have a backup process in place?
- Is my local backup checked regularly to make sure it works?

POPIA encourages you to rethink your data security environment and business processes, and reinforces best practices which will support not only your compliance with the Act, but will support your business efficiency and growth too.



Actions that cannot wait.

1. Register your practice's Information Officer on https://www.justice.gov.za/inforeg/portal.html
2. Draft and implement a general POPIA policy, and post it on your practice's website, if you have one.
3. Draft and implement a PAIA policy, and post it on your practice's website, if you have one.
4. Sign data privacy agreements with each practice staff member and third-party provider.
5. Record each patient's consent for the practice to process and share their personal information.
6. Educate practice staff about your new POPIA-aligned procedures.

In any organisation, ultimate the head of the organisation is the registered Information Officer, and is responsible for privacy, but he/she can appoint a Deputy Information Officer or so-called Privacy Officer or suitably qualified person to oversee POPIA implementation.

For more information on POPIA visit **www.cgm.com/za-popia2021**

Manage data privacy in your practice.

Get Consent

Get written consent from each of your patients confirming their consent for your practice to:

- Process their personal information and in particular, their health information.
- Share their personal information and health information with third party operators for the specific purpose of supporting the doctor's provision of an integrated health treatment service to them.

Reminder: If patients refuse to give permission for sharing of their health information with medical schemes or other insurers, the third party may refuse to pay their claim.

Third party operators can be medical schemes, medical facilities, insurers, administrators, other medical practitioners, pharmacies, and electronic service providers – like CGM.

Request Patient Consent Template

Privacy Agreements

Ensure that you have data privacy agreements in place with all your staff, and all third-party operators who may process or further process your patients' personal information.

Only allow access to staff who have signed Data Security Agreements, and then only allow access to the specific elements of personal information needed to fulfil their specific purpose.

Request Privacy Agreement Templates

Reduce Your Paper Records

- Shred any excess documents containing personal information.
- Make secure soft copies your first option.
- If you don't need it anymore, and aren't obliged to keep it by law (remember the 6-year rule), shred it.
- Store paper documents containing personal information securely.

Manage data privacy in your practice (cont.)

Password Protection

- Ensure that each staff member has their own password, which is strong enough, and is securely stored.
- Passwords should be at least 10 characters, including a mixture of upper case and lower-case letters, numbers, and special characters.
- DO NOT share or write passwords down where they can be easily accessed or located.

Lock it Down

Restrict access to patient files:

- Only the treating healthcare practitioner should have access to a patient's health records at your practice.
- Reception, accounts, and administrative staff should ONLY have access to patients' contact details, account information, and medical scheme numbers – not the complete patient file.

Backup Your Data

- Put procedures in place for making backups of your practice data.
- If you do not use a cloud-based service, then you need to make at least 2 daily back-ups, one of which must be stored off-site. Your back-ups must be checked regularly to ensure that they actually work and are not corrupted.
- Talk to your IT provider or contact CGM to make sure your backups are up-to-date.

Contact CGM for my data backups

For more information on POPIA visit **www.cgm.com/za-popia2021**

Manage data privacy in your practice (cont.)

Update Your Software

Updates are important! They might fix existing security holes and computer bugs and help you to protect your data. And additionally, they will add new features to your software.

Ensure your updates are done on time and that your IT provider has installed adequate cybersecurity on your system, work-stations, and all connected devices in the form of firewalls, anti-virus and anti-malware software.

Conduct Reguar Audits

New procedures are only good if they are being applied and further developed. Check regularly with your staff if the new policies are being applied and reiterate the most important ones.

Every time you deal with Personal Information ask yourself:

- Have I collected only the minimum information I need?
- Is the information securely stored while it is in my practice?
- Do I have the patient's permission to process their information?
- Is processing without the patient's permission allowed because it is in the patient's interests to share the information?

For more information on POPIA visit **www.cgm.com/za-popia2021**

Think Privacy.

CompuGroup Medical SA (Pty) Ltd.

3 Century City Drive · Century City · Cape Town · 7441 · South Africa
P: 0861633334 · E: hello.za@cgm.com · www.cgm.com/za-popia2021
Directors: Christo Groenewald · Thorsten Kollet
Company domiciled in: Cape Town
Company Reg. No. 2005/023029/07 · VAT ID: 432 022 6063

Synchronizing Healthcare

CompuGroup Medical