The five practice controls

Patient confidentiality was always a clinical duty. In a digital practice it rests on these five controls.

1. **Verify before you send**
   Confirm the recipient every time patient information leaves by WhatsApp or email. Stop clinical photos saving to the phone gallery.

2. **Lock the accounts**
   Two-step verification on practice email and WhatsApp. No shared logins. Leavers removed the day they go.

3. **Know who holds your patient data**
   A written list of every outside company that processes it, each with a written contract (POPIA s21).

4. **Own the first hour**
   A named Information Officer, registered with the Information Regulator (s55), and written first-hour steps (s22).

5. **Be able to keep working**
   One backup that is offline or can't be altered, a test restore every quarter, and a paper fallback pack.

SCORE YOUR PRACTICE · COUNT YOUR YESES

- [ ] Two-step verification on the practice email and WhatsApp?
- [ ] A rule for checking the recipient before patient information is sent?
- [ ] A written list of every outside company holding your patient data?
- [ ] A registered Information Officer and written first-hour steps?
- [ ] An offline backup, test-restored in the last three months?

POPIA s19 (security safeguards), s21 (operators), s22 (notification), s26 (special personal information), s55 (Information Officer); National Health Act s14 (confidentiality) and s17 (protection of health records).

Front desk: before patient information leaves

For reception, practice managers and anyone who answers the phone or the practice WhatsApp.

1. **Check the recipient against the file — every time**
   Read the number or address back before you press send. Numbers in files go stale.

2. **Callers asking for results: take a reference, call back**
   End the call and phone back on the number in the patient's file or the scheme's published number. An ID number doesn't prove who is calling.

3. **Never send to a number or address the caller gives you**
   If it isn't already on file, it isn't verified.

4. **Keep clinical photos off the gallery**
   Android: three-dot menu → Settings → Chats → Media visibility off. iPhone: Settings → Chats → Save to Photos off. Delete images from the phone once filed in the record.

5. **Your own login, locked when you step away**
   No shared passwords at the front desk.

6. **Something went to the wrong place? Say so the same hour**
   Telling the Information Officer quickly is the duty. Silence is the violation.

WHO TO TELL

Information Officer: _____

Cell: _____

The first hour

If patient information may have been seen by someone who shouldn't have it, follow these steps in order.

1. **Stop**
   Send nothing else. Don't try to fix it quietly.
2. **Contain**
   Ask for a misdirected message to be deleted; recall it if you can. Disconnect an affected device from the network — don't switch it off.
3. **Preserve**
   Screenshots, times, who sent what to whom. Delete nothing.
4. **Record**
   Write it down below while it's fresh.
5. **Escalate**
   To the Information Officer, the same hour.
6. **Assess**
   Whose information, how sensitive, who could now see it.
7. **Notify**
   The Information Regulator and the affected patients, as soon as reasonably possible (POPIA s22). Report to the Regulator through its eServices portal — mandatory since 1 April 2025.

INCIDENT RECORD

Item	Details
Discovered (date, time, by)	
What happened	
Whose information	
Actions taken	
Regulator notified on	
Patients notified on (how)	

When the systems go down

In June 2024 ransomware hit the NHLS and deleted sections of its systems — including in its backup server. Most practice backups sit on the same network as everything else.

BEFORE IT HAPPENS

- [ ] One backup that is offline or can't be altered
- [ ] Paper fallback pack in a drawer: printed day list, blank clinical notes, script pads
- [ ] Key numbers off the computer: labs, medical schemes, IT support, practice owner
- [ ] A claims plan: how claims are captured now and submitted once systems return
- [ ] Staff know where the pack is and who decides to switch to paper

QUARTERLY TEST-RESTORE LOG · UNTESTED, YOU DON'T KNOW YOU HAVE A BACKUP

Date	What was restored	Worked?	Restored by

Sources: NHLS statement via SAnews (26 Jun 2024); Life Healthcare reported patient billing, medical-aid claims and supplier invoices affected during June and part of July 2020 (ITWeb, 31 Aug 2020).

10-minute staff huddle

Run this at a Monday staff meeting. Read the scenario, ask the questions, agree the rule, sign.

READ ALOUD

A caller says they're from a patient's medical aid. They need the latest results urgently to approve a claim, and they can give you the patient's ID number.

ASK THE TEAM — HONESTLY

1. **What would each of us do right now?**
2. **Does the ID number prove who is calling?**
3. **Which number would we call back — and where is it?**
4. **Who do we tell if information has already gone out?**

OUR RULE FROM TODAY

_____

_____

ATTENDANCE · KEEP THIS SHEET AS YOUR TRAINING RECORD

Date: _____

Led by: _____

Name	Role	Signature