INNOVO NETWORKS · FREE SELF-AUDIT TOOL

# The POPIA & Ransomware Risk Checklist

A 10-minute self-audit for SouthAfrican health care practices— GPs, dentists, pharmacies, specialists, clinics & hospitals.

INNOVO NETWORKS
THINK SOLVE CONNECT

**Why this matters:** POPIA violations can carry fines of up to R10 million and criminal liability for directors. South Africa is the most targeted country in Africa for ransomware, with healthcare facing 1,600+ attacks a week. Most practices don't discover their exposure until something has already gone wrong.

**How to use this:** Tick every box that reflects your practice today. Each unticked box is a potential exposure point. Score yourself at the end.

## 1 DATA PROTECTION & POPIA

- ☐ We know exactly where patient data is stored and who can access it.— *unknown data flow = audit risk*
- ☐ We have a documented, tested breach-notification process. —*required under POPIA*
- ☐ Patient data is encrypted both in transit and at rest.—*unencrypted= direct violation*
- ☐ We produce regular (monthly/quarterly) compliance reporting. —*most practices produce none*
- ☐ Staff have received POPIA awareness training in the last 12 months. — *human error is the #1 cause of breaches*

## 2 COMMUNICATIONS & CALL SECURITY

- ☐ Our phone calls are encrypted end-to-end (not just internet traffic).— *legacy PBX = eavesdropping risk*
- ☐ Call recordings (if used) include POPIA-compliant consent prompts. — *unconsented recording = violation*
- ☐ After-hours and emergency calls are routed reliably, every time. — *gaps here = missed emergencies*
- ☐ We can produce a full audit log of call activity on demand. —*needed for compliance & billing disputes*

## 3 NETWORK & DEVICE SECURITY

- ☐ Medical IoT devices (scanners, monitors, pumps) sit on an isolated network segment. — *flat networks = single point of failure*
- ☐ We have ransomware defence with automatic endpoint isolation. — *not just antivirus*
- ☐ We monitor the dark web for our patients' leaked data or credentials. —*most breaches are discovered too late*
- ☐ We have a next-gen firewall with intrusion detection tuned to healthcare threats.—*generic firewalls miss healthcare-specific attacks*

# The POPIA & Ransomware Risk Checklist

A 10-minute self-audit for SouthAfrican health care practices— GPs, dentists, pharmacies, specialists, clinics & hospitals.

## 4 BUSINESS CONTINUITY & LOADSHEDDING

- ☐ Our internet and phones stay online automatically during load shedding. *—no failover = downtime during outages*
- ☐ A single device or connection failure would not take down the whole practice. *—no redundancy = cascading failure*
- ☐ We have one accountable provider for internet, phones and security — not three. *— fragmented vendors = slower fixes, more finger-pointing*

### SCORE YOURSELF

**15-17 boxes ticked:** Strong position. Worth a professional audit to confirm and document it.
**9-14 boxes ticked:** Meaningful gaps exist. These are exactly the gaps that turn into fines or downtime.
**Below 9 boxes ticked:** Significant exposure. We'd recommend a full risk assessment as a priority.

## Want the professional version of this audit — free?

**Book a free 30-minute HealthShield™ Risk Assessment.**

We'll review your actual environment — internet, phones and network — and show you exactly what's at risk. No cost, no obligation.

087 291 7557 · sales@innovonet.co.za · www.innovonet.co.za