

The Ultimate PLAYBOOK for Selling ComplianceSuite™ to Medical Practices in South Africa.

The functional equivalent that bridges international information security standards with local legal requirements is a combination of **POPIA (Protection of Personal Information Act) Compliance** supported by **ISO/IEC 27799** (specifically for health informatics).

This document aims provide **SMBsecure ASP** sales teams with knowledge and understanding to develop a winning strategy for targeting Medical Practices in South Africa and how to converse with practice managers about **ComplianceSuite** benefits.

***Disclaimer:** While these guidelines are based on HPCSA and POPIA requirements, it is recommended to seek legal advice or specialized consulting to ensure full compliance for a customer's specific practice.*

The Basics....

The HPCSA mandates that patient records be stored in a safe place, and if in electronic format, safeguarded by effective, industry-standard measures.

The Core Regulatory Framework

To meet HPCSA, National Health Act, and POPIA requirements, South African medical practices must adopt a framework that covers:

- **POPIA Compliance (Law):** Mandatory since 1 July 2021, governing how personal and special personal information (health data) is collected, processed, stored, and destroyed.
- **ISO/IEC 27799:2008 (Information Security for Health):** The HPCSA specifically references this standard for managing information security in health institutions. This standard acts as a guideline on how to apply ISO 27002 controls within a health context.
- **HPCSA Ethical Guidelines (Booklet 5 & 10):** These stipulate that practitioners must ensure appropriate, reasonable technical and organizational steps to protect patient data, including during tele-health.

Key Requirements for Compliance

To align with these standards, practices must implement the following:

- **Secure Storage & Access Control:** Electronic data must be password-protected, encrypted, and accessible only to authorised personnel.
- **Staff Training:** Receptionists and clerks must be trained on patient confidentiality, scams and attacks targeting medical practices, and safe patient data handling.
- **Data Minimisation & Accuracy:** Only relevant, necessary information should be collected.
- **Retention Policy:** Records must generally be kept for at least **six years** after they become dormant, or longer for minors and incapacitated patients.
- **Secure Disposal:** Digital and physical records must be destroyed in a manner that prevents reconstruction.
- **Information Officer:** Designation of an Information Officer to oversee compliance.

Summary of Compliance Actions

Requirement	Action Required
Legal	Ensure compliance with POPIA Act and National Health Act.
Security Standard	Implement ISO/IEC 27799 (Health informatics) for managing data.
Record Keeping	Adhere to HPCSA Booklets 5 & 10 (Confidentiality & Telehealth).
Risk Management	Identify potential breaches, secure patient terminals, and use encryption for data transmission and storage.

For healthcare-specific information security management, the **HPCSA** explicitly references **ISO 27799:2016** as the internationally accepted standard to follow for managing and backing up electronic data.

The regulatory framework for security in South African medical practices includes:

1. HPCSA Ethical Guidelines

The HPCSA provides specific "Booklets" that define the standards for data protection:

- **Booklet 9: Guidelines on the Keeping of Patient Records:** Requires electronic data to be managed, stored, and backed up using internationally accepted standards like **ISO 27799**.
- **Booklet 5: Confidentiality: Protecting and Providing Information:** Outlines the duty to ensure appropriate security arrangements for information stored or sent by electronic means.
- **Booklet 10: Telehealth:** Provides detailed security requirements for remote patient interactions and data transmission.

2. Statutory Compliance (POPIA & PAIA)

These acts are the legal backbone for information security in South Africa and align closely with ISO 27001's risk management approach:

- **POPIA (Protection of Personal Information Act):** Mandates "reasonable technical and organisational measures" to prevent loss, damage, or unauthorised access to personal data.
- **PAIA (Promotion of Access to Information Act):** Requires practices to maintain a manual (often combined with a POPIA policy) detailing how information is protected and accessed.

3. Key Technical Requirements Prescribed by HPCSA

While not a formal "certification," the following controls are mandatory for compliance:

- **Access Control:** Individual passwords for all staff; generic passwords are not permitted.
- **Encryption:** Mandatory for all clinical records stored on portable media (e.g., USB drives) and recommended for electronic transmissions (email encryption).
- **Backups:** Regular backups must be kept at a secure, physically separate off-site location.
- **Audit Trails:** Electronic records must be attributable, meaning any person making an entry must be identifiable and the entry must be dated and timed.

For medical device manufacturers or establishments (rather than general practices), **ISO 13485** (or the equivalent **SANS 13485**) is often a mandatory legal requirement under SAHPRA.

A Simple Checklist:

This checklist combines the **HPCSA Booklet 9** (Patient Recordkeeping) and **POPIA** requirements to help a practice align with the data security objectives of ISO 27001.

1. Governance and Accountability (POPIA)

- **Appoint an Information Officer:** Formally designate a person responsible for compliance and register them with the Information Regulator.
- **Maintain a PAIA Manual:** Ensure you have a current Promotion of Access to Information Act manual available to the public.
- **Establish a Data Inventory:** Document what personal and medical information you collect, where it is stored, and who has access.
- **Operator Contracts:** Ensure written agreements are in place with third-party providers (e.g., cloud storage, billing bureaus, debt collection) to guarantee they are POPIA compliant and also safeguard any patient data shared with them.

2. Clinical Record Security (HPCSA Booklet 9)

- **Access Control:** Ensure every staff member has a unique, individual login; generic "reception" or "admin" passwords are prohibited.
- **Attributability:** Verify that every entry in an electronic record is automatically dated, timed, and linked to a specific identifiable user.
- **Integrity of Records:** Use systems that prevent original entries from being deleted or overwritten. Alterations must be made as a new, dated, and signed note.
- **Encryption:** Confirm all electronic clinical records, especially those on portable media like USBs or sent via email, are password-protected and encrypted.
- **Off-site Backups:** Ensure backups are regular and stored in a physically separate, secure location from the primary data. Recovery must be tested.

3. Patient Privacy and Consent

- **Privacy Notice:** Display a clear notice in your waiting room or on your website explaining how you use patient data.
- **Informed Consent:** Explicitly obtain and record patient consent before collecting data or using telehealth services.

SMBsecure™

- **Data Minimality:** Only collect information that is strictly necessary for the clinical purpose or legal requirement.
- **Retention Schedule:** Implement a policy to delete or de-identify data after the mandatory retention period (typically **6 years** for adults, or until age **21** for minors).

4. Technical and Physical Safeguards

- **Network Security:** Use updated firewalls, anti-virus software, and VPNs (secure connections) for any remote access.
- **Physical Security:** Lock physical filing cabinets and ensure offices where servers or records are kept are secured.
- **Breach Response Plan:** Have a documented procedure to notify the Information Regulator and affected patients immediately if a data breach occurs.
- **Staff Training:** Conduct regular training sessions for all employees on handling patient information securely.

POPIA Compliance for Medical Practices Made Simple...

Elevator Pitch

ComplianceSuite™ helps doctors, clinics, and healthcare providers manage patient data protection, regulatory compliance, and governance with a structured & practical solution and effective measures.

The Challenge

Medical practices handle highly sensitive personal information, including patient medical records, identification details, and billing information.

Under South Africa's Protection of Personal Information Act (**POPIA**), healthcare providers must ensure that patient data is:

- Collected lawfully
- Stored securely
- Protected from unauthorised access
- Managed responsibly across staff and systems

Many practices struggle with these requirements due to limited time, resources, and compliance expertise.



The ComplianceSuite™ for Medical Practice Solution

ComplianceSuite™ provides an **All-in-One** solution to help medical practices:

- ✓ Manage POPIA compliance requirements
- ✓ Protect patient information
- ✓ Maintain compliance documentation
- ✓ Track risks and controls
- ✓ Prepare for audits and regulatory reviews

Key Benefits for Medical Practices

Protect Patient Data

Implement structured processes for safeguarding sensitive medical information.

Simplify POPIA Compliance

Manage compliance obligations through guided frameworks and workflows.

Improve Governance and Accountability

Ensure policies, procedures, and controls are documented and maintained.

Reduce Administrative Burden / Maintain Audit Readiness

Automate compliance tasks so healthcare professionals can focus on patient care.

ASP Email Campaigns for Medical Practices

Email 1 – Awareness

Subject - Is your medical practice really POPIA compliant?

Dear Doctor / Practice Manager,

Medical practices handle some of the most sensitive personal information — patient medical records.

Under South Africa’s Protection of Personal Information Act (**POPIA**), healthcare providers are required to ensure patient information is properly protected and managed.

Unfortunately, many practices are unsure whether their current processes meet these regulatory requirements.

To help medical practices better understand their obligations, we’ve prepared a simple **POPIA + Cybersecurity Compliance Checklist for Medical Practices**.

[Download it here:](#)

[Insert link]

The checklist will help you quickly assess whether your practice has the policies, controls, and governance processes needed to protect patient information.

Kind regards

[Name]

Email 2 – Education

Subject - Common POPIA risks facing medical practices

Dear Doctor / Practice Manager,

Many medical practices unknowingly face POPIA compliance risks when managing patient information.

Some of the most common risks include:

- Unsecured patient records
- Limited staff awareness of privacy requirements
- Weak access controls for patient information
- Lack of documented compliance procedures



These issues can expose practices to regulatory scrutiny and reputational risk.

ComplianceSuite™ helps healthcare providers implement structured compliance management processes that simplify POPIA + Cybersecurity compliance and protect patient information.

If you would like to learn more, we invite you to attend our upcoming **POPIA + Cybersecurity Compliance for Medical Practices webinar**.

[Register here]

Kind regards

[Name]

Email 3 – Offer

Subject - Free POPIA + Cybersecurity compliance assessment for medical practices

Dear Doctor / Practice Manager,

Understanding whether your medical practice is POPIA compliant can be challenging.

To help healthcare providers navigate these requirements, we are offering a **complimentary POPIA + Cybersecurity compliance assessment for medical practices**.

During the assessment we will help you:

- Identify potential compliance gaps
- Review patient data protection practices
- Provide practical recommendations for improving compliance

Following the assessment, we will also show how **ComplianceSuite™** can help your practice manage compliance more effectively.

To schedule your assessment, simply reply to this email or contact us here:

[Insert contact link]

Kind regards

[Name]

ComplianceSuite™ | Healthcare Sales Kit

Target Healthcare Segments

ComplianceSuite for Healthcare supports:

- General Practitioner practices
 - Specialist practices
 - Clinics
 - Day hospitals
 - Medical groups
 - Healthcare administrators
-

Talking Points

SMBsecure ASP sales teams may consider conversation angles such as:

- POPIA compliance challenges in healthcare
 - Protecting patient information in private medical practices
 - Governance and compliance for healthcare providers
 - Cybersecurity risks in healthcare environments
-

Building Your MSP Healthcare Services

SMBsecure Objective

Enabling you, our Authorised Service Provider to deliver **POPIA + Cybersecurity compliance services to medical practices** using **ComplianceSuite**.

Disclaimer: While these guidelines are based on HPCSA and POPIA requirements, this is NOT A LEGAL ENGAGEMENT by you! It is recommended for your customer to seek professional legal advice or specialized consulting to ensure full compliance for a customer's specific practice.

“Guidance” or “Services” You Can Offer

ASPs can deliver:

- **POPIA Compliance Assessments**
Evaluate whether a practice meets regulatory requirements.
 - **Compliance Implementation**
Develop policies and procedures required for POPIA compliance.
 - **Compliance Monitoring**
Provide ongoing compliance oversight and reporting.
 - **Data Protection Governance**
Support healthcare providers in managing patient information responsibly.
-

Revenue Opportunities

You can generate recurring revenue through:

- Compliance assessments
 - Compliance consulting
 - Compliance monitoring subscriptions
 - Governance advisory services
-

Example ASP Service Packages

Starter Package

- POPIA compliance assessment
- Compliance checklist review

Professional Package

- Compliance framework implementation
- Staff awareness training

Managed Compliance Package

- Continuous compliance monitoring
- Quarterly compliance reviews
- Compliance reporting

Strategic Positioning (Recommendation)

To dominate the healthcare compliance market, position the product as:

“ComplianceSuite – The POPIA Compliance + Cybersecurity Solution for Medical Practices.”

This positioning is powerful because:

- POPIA is the **primary regulatory concern for medical practices**
- Doctors understand **patient confidentiality risk**
- ComplianceSuite becomes the **obvious solution**

Below is a **practical ASP Healthcare Sales Script** your partners can use when selling **ComplianceSuite to medical practices in South Africa**.

It is designed to work as a **10–15 minute discovery conversation** that quickly surfaces POPIA risks and naturally leads to a ComplianceSuite discussion.

ComplianceSuite Healthcare: Sales Script for ASPs

Objective

These scripts are designed to help ASP partners start conversations with doctors and clinic managers about protecting patient data and complying with the POPIA, while positioning ComplianceSuite as the structured solution.

1 Opening Conversation (2 minutes)

Goal: Introduce the topic in a way that resonates with doctors.

Example introduction

“Many medical practices we speak to are concerned about protecting patient information and ensuring they meet the requirements of the HPCSA & Protection of Personal Information Act.

Because practices store highly sensitive patient data, regulators and medical aids expect them to demonstrate responsible data protection and governance.”

Follow-up question:

“Has your practice done a POPIA + Cybersecurity compliance assessment yet?”

Possible answers:

- **Yes** → ask about documentation and processes, audit readiness, policy effectiveness, and (importantly) about technical controls implemented
 - **No / Not sure** → move to discovery questions
-

2 Discovery Questions (5 minutes)

The goal here is to identify **compliance gaps** without sounding overly technical.

Governance

Ask:

“Has your practice formally appointed and registered an Information Officer?”

POPIA requires all organisations processing personal information to designate an Information Officer.

Policies

Ask:

“Do you currently have documented privacy policies, PAIA Manual and procedures for handling patient information?”

Most small practices **do not** have this documented and readily available.

Patient Records

Ask:

“How are patient records stored today — electronically, physically, or both?”

Follow up with:

“And who in the practice has access to those records?”

“Is all that data fully encrypted on devices that have it, and are those devices secured?”

This helps reveal access control gaps.

Staff Awareness

Ask:

“Have staff members received any training on scams, potential risks, properly protecting patient information or POPIA responsibilities?”

This is a **major compliance gap** in healthcare.

Incident Response

Ask:

“If patient information were accidentally disclosed or compromised, do you have a process for reporting and managing that incident?”

Most practices **do not have a breach response process**.

Third Party Compliance

Ask:

“Do you make you of external 3rd party billing bureaus, debt collectors or outsourced HR for your medical practice? Are they compliant? Have you checked?”

This is a **major compliance gap** in healthcare placing your practice at-risk.

3 Position the Risk (2 minutes)

After discovery, summarise what you heard.

Example:

“What we see across many medical practices is that while patient information is handled carefully, there often isn’t a structured compliance framework in place for POPIA, and effective (provable) technical safeguards for that data.”

Explain the risks:

- Data breaches, scams, cyber-attacks
- Regulatory scrutiny
- Patient trust concerns
- Scam & fraud vulnerabilities / targeting

SMBsecure™

- 3rd party risks (billing bureaus and debt collections)
- Lack of documentation during investigations

Healthcare providers must demonstrate responsible data governance.

4 Introduce ComplianceSuite (3 minutes)

Now position the solution.

Example explanation:

“To help practices address these challenges, we provide a solution bundle called ComplianceSuite.”

ComplianceSuite helps practices:

- ✓ Manage POPIA compliance
- ✓ Document policies and procedures
- ✓ Track compliance activities
- ✓ Maintain audit-ready documentation
- ✓ Implement robust technical measures and governance processes

Explain the value simply:

“It gives medical practices a structured capability for managing compliance + cybersecurity in-one, instead of trying to track everything manually.”

5 Offer a Compliance Assessment (**Close**)

The goal is **not to sell immediately** but to offer an assessment.

Example:

“The first step we normally recommend is a short & quick POPIA compliance assessment for the practice.”

Explain the outcome:

During the assessment we:

- Review how patient information is handled
- Identify potential compliance gaps
- Provide practical recommendations

Then say:

“From there we can show how ComplianceSuite helps manage compliance going forward.”

Call to Action

Offer two simple options:

Option 1

“Would you like us to schedule a short POPIA compliance assessment for your practice? It will only take 15 minutes”

Option 2

“I can also send you our POPIA compliance checklist for medical practices if you'd like to review it internally first.”

Why This Script Works

This approach works because it:

- ✓ Focuses on **patient data protection**
 - ✓ Uses **simple language doctors understand**
 - ✓ Avoids heavy technical compliance jargon
 - ✓ Positions you - *the ASP* - as a **trusted advisor**
-

Strategic Opportunity

Very few vendors currently provide **structured POPIA + Cybersecurity compliance solutions for medical practices**. Positioning ComplianceSuite™ as:

“***The POPIA + Cybersecurity Compliance Solution for Medical Practices.***” could make it the **default compliance bundle for healthcare providers in South Africa**.

Pro Tip

Combine a basic POPIA Compliance Risk Assessment *plus* FREE External Scan (Telivy) “Executive Summary Report” and DMARC Scan (if they have a domain) for a powerful consultative prospect engagement!

POPIA Compliance Risk Calculator for Medical Practices




Doctors answer **10 questions**, and it produces a **risk score** and recommendation for ComplianceSuite. This tool is **incredibly effective for lead generation and sales conversations**.



ComplianceSuite_Hea
lthcare POPIA Risk Cal

What this tool does

This Excel sheet allows you to:

- Assess a medical practice against **10 key POPIA requirements**
- Generate an automatic **compliance score**
- Instantly classify the practice as:
 -  High Risk
 -  Moderate Risk
 -  Lower Risk

Branded & Structured

- Clear **ComplianceSuite positioning**
- Clean layout for client-facing use
- Proper report flow (Details → Score → Summary → Recommendations)

Smart Automation Built-In

- Auto-calculates **Risk Level**
- Auto-generates:
 - Executive Summary
 - Recommendations
- Language is **clean, client-ready and professional**

Presentation-Ready Report Tab

- Designed to:
 - Show live in meetings
 - Export / Print to PDF
 - Send directly to clients

How to use it in sales (very powerful)

During a meeting:

1. Ask the doctor or practice manager the 10 questions
2. Fill in scores (0 / 1 / 2) live
3. Show the total score instantly

Then say:

“Based on this, your practice currently falls into the **[risk level]** category. What we typically do next is help practices close these gaps using a structured solution like ComplianceSuite.”

How to turn this into a lead engine

You can also use this as:

Website Tool

“Check your POPIA Compliance Score in 2 minutes”

Webinar Hook

“Complete your compliance score during the session”

Sales Trigger

Any score below 16 = strong ComplianceSuite opportunity

Pro Tip (High Conversion)

Add this positioning when presenting results:

“Most medical practices we assess fall into the moderate to high-risk category — not because they’re doing things wrong, but because they don’t have a structured compliance framework in place.”

This removes defensiveness and increases conversion.

How to position it (very important)

When presenting the report, say:

“We’ve completed a basic but structured POPIA assessment of your practice. This report highlights your current compliance position and the key areas that need attention.”

Then say:

“Based on your assessment, this is your current POPIA compliance position.”

 This feels like a **formal advisory engagement**, not a sales pitch.

What makes this powerful

This turns your conversation into:

- A **professional consulting engagement**
 - Not just a sales discussion
 - Positions you as a **compliance advisor**, not a vendor
-

Conversion Strategy (Proven)

End the report walkthrough with:

“Based on these findings, the next step is to implement a structured compliance framework. That’s exactly what ComplianceSuite is designed to support.”

Turn this into a scalable revenue engine

With this tool, you can now deliver:

Paid Assistance / Engagements

Professional services = **billable service**

- Upgrade OS *-> If running home/SL*
- Refresh Hardware *-> Still running Windows10*
- Migrate to a domain / M365 *-> If no domain or not on M365*
- Penetration test *-> If larger entity*
- Establish policies & procedures, etc. *-> For improved governance*

Recurring Revenue

Position ComplianceSuite as:

“The solution to manage this continuously”






High Conversion

Because the client now:

- Sees their risk
- Understands the gap
- Wants a structured solution

Why this tool is extremely powerful

You now have:

-  Assessment tool
-  Automated analysis
-  Auto-generated report
-  Consulting framework
-  Sales conversion engine




 This is **consulting-grade tooling**, not just marketing material.

Pro Tip (Use this exact close)

After showing the report:

“What we’ve done here manually is exactly what ComplianceSuite automates and manages on an ongoing basis.”

This bridges perfectly into:

-  Subscription
-  Managed compliance
-  Long-term revenue

Pitching and Selling to “Micro” Medical Practices

Many small medical practices in South Africa are actually Micro enterprises i.e. 1-3 computers or users. This presents a massive opportunity to sell **ComplianceSuite Micro** as a low-cost solution for compliance and security governance to these micro-sized practices.

A Professional Indemnity (PI) Policy generally excludes cybercrime-related theft. Practices must obtain standalone cyber liability insurance to cover data breaches and fraudulent transfers.

Note: ComplianceSuite Cyber Warranty only provides 1st party protection (our customer)

Typical Profile for ComplianceSuite™ MICRO

- ✓ 1-3 Computers / Users (Max)
- ✓ Very busy professional
- ✓ Friendly towards “Compliance”
- ✓ High awareness about POPIA
- ✓ Have only basic technical measures
- ✓ Might not even have a domain, uses Gmail (etc) for email communications
- ✓ Unaware of required technical & organisational measures
- ✓ High target for Scams, Attacks & Data Breach

ASP Benefits

With this PLAYBOOK, you now have a **complete vertical go-to-market for healthcare:**

- Positioning/Understanding ✓
- Focussed Targeting ✓
- Lead magnets ✓
- Webinar ✓
- Sales deck ✓
- Sales script ✓
- Risk calculator ✓
- Report generator ✓
- Brandable whitepaper ✓ *(Text Copy on next page)*

■ **Whitepaper:** POPIA Compliance for Healthcare Providers

👉 *Copy below text to a new word document with your logo and save to PDF!*

Title

Protecting Patient Information:

POPIA + Cybersecurity Compliance for Medical Practices in South Africa

Executive Summary

Healthcare organisations handle some of the most sensitive personal information, including patient medical records, identification details, and clinical history. Ensuring the privacy and security of this information is essential for maintaining patient trust and complying with regulatory obligations.

South Africa's Protection of Personal Information Act requires healthcare providers to implement appropriate safeguards to protect personal information and ensure responsible processing of patient data.

However, many medical practices lack the resources, processes, and tools required to manage compliance effectively.

The Healthcare Data Protection Challenge

Medical practices process large volumes of sensitive information such as:

- Patient personal information
- Medical history
- Diagnostic records
- Billing and insurance information

Without proper governance and controls, this information can be exposed to risks such as:

- Unauthorised access
- Data breaches, scams and fraud
- Improper data sharing
- Inadequate record management

Regulatory Expectations

Healthcare providers must ensure that patient information is:

- Collected lawfully
- Used for legitimate healthcare purposes
- Protected against unauthorized access
- Stored securely
- Retained according to policy

Failure to comply may result in regulatory investigation and reputational damage.

Best Practices for POPIA Compliance in Medical Practices

Healthcare providers should implement:

Information Governance

Assign responsibility for privacy and information protection.

Data Protection Policies

Document procedures for managing patient data.

Access Control

Ensure only authorised staff can access sensitive patient information.

Staff Awareness

Train staff on privacy and data protection responsibilities.

Security Controls

Protect patient data from cyber threats and unauthorised access.

How ComplianceSuite™ Supports Healthcare Providers

ComplianceSuite™ provides a practical solution for managing compliance activities across healthcare organisations.

The solution bundle helps medical practices:

- Manage compliance frameworks
- Implement essential technical & organisational measures (TOMs)
- Track risks and controls
- Maintain documentation
- Prepare for regulatory audits
- Monitor compliance status