SMBsecure™ HCP ComplianceSuite

50+ Controls Checked For Your Cybersecurity Compliance.

Reduce COST

Reduce. COMPLEXITY

Improve COMPLIANCE

SME VALUE

Great Value Cybersecurity Compliance

> 50+ Controls Checked + Dark Web Monitoring.
> Crucial Layers of Data Protection Addressed.
> NIST/ISO/CIS CSF Compliance Assessments.
> R1M Cyber Warranty.

> **POPI Toolkit.**

BONUS:

+ Live AI Assistant & Compliance Tracker.
+ FREE Policy Templates.

What Is Cybersecurity Compliance?

Cybersecurity compliance is your adherence to security and data protection guidelines (such as HPCSA code of conduct), regulations (such as the POPI Act, PAIA, GDPR, etc), Frameworks and Standards (such as NIST, CIS, ISO27001, etc) or those data security questionnaires which you might be asked to complete by suppliers and customers for business engagement. These regulations, frameworks and questionnaires are significant to ensuring that your organisation's security practices align with legal and industry requirements, thereby mitigating risks and maintaining trust.

Why You Need To Comply with POPIA & PAIA Regulations?

In the current landscape of ever-present and evolving digital threats and scams, it is crucial for your practice to demonstrate a strong commitment to cybersecurity compliance to build trust with patients, partners, and stakeholders, and enhance your practice's reputation. In South Africa, the Protection of Personal Information Act (**POPIA**) is an important requirement set by government to regulate the collection, use, protection, security and disposal of personal information of S.A. citizens and companies – both are recognised under the law. Equally the Promotion of Access to Information Act (**PAIA**) helps to protect internal and confidential data when access requests are made. Compliance is not merely a regulatory burden; it is a fundamental aspect of responsible business practice. Complying with POPIA & PAIA are essential for protecting your patients, your own practice, and the supply-chain. The Information Regulator has been empowered by these Acts to enforce the regulations. Non-compliance can lead to severe penalties, including **Substantial Fines**: The regulator has the authority to levy significant financial penalties for data breaches. **Enforcement Action:** This can range from mandated remedial actions to public notices causing **reputational damage and patient defection**.

How To Implement Cybersecurity Compliance?

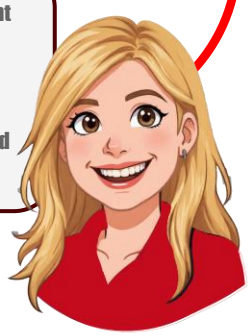
As a practice owner you must embed the security of personal information into your practice culture. This means treating compliance not as an IT project, but as a core, ongoing business function focused on managing risk, protecting sensitive data and **implementing security controls**.

How SMBsecure™ Helps With Cybersecurity Compliance?

SMBsecure™ simplifies and enhances cybersecurity for small and mid-sized health practices, helping to meet several key requirements for cybersecurity compliance. It inexpensively offers broad coverage for compliance that includes data protection, risk assessment, external & internal attack surface monitoring, vital controls, reporting and auditing, and employee training. **ComplianceKate®** is your personal AI Assistant to guide you through everything. It's all backed with a Cyber Warranty to provide remediation & financial peace-of-mind. This all leads to **lower risk**, **improved compliance**, **increased operational efficiency** and **Trust**.

Cost Effective, All-in-One Cybersecurity Compliance

Hi, I'm Kate. Your AI Assistant here to help you with questions, scenarios, templates and guidance related to Data Protection, POPIA, PAIA, Frameworks and SMBsecure™ info.



SMBsecure™ | HCP ComplianceSuite

www.smbsecure.co.za

www.compliancesuite.co.za

Get Data Security & Compliance
as part of your everyday data processing…

HOW IT WORKS

The ultra affordable **SMBsecure™** ComplianceSuite leverages patented technologies from leading and world class technology vendors that can be deployed in minutes to address cybersecurity compliance and make securing data on PCs, Macs, USBs, Mobiles and Emails a **Total Breeze.**

Your Health Practice Is Built On Trust

Patients entrust you with their sensitive personal and medical information, as well as their hard-earned money. A successful cyberattack can lead to scams, theft of personal data and funds, identity theft, significant financial loss and emotional distress to patients. **SMBsecure™** ensures that your practice will have robust security measures in place to protect sensitive and personal information from unauthorised access & disclosure.

A Cyber Incident Can Be Costly For Your Health Practice

The consequences can include:

> **Financial Loss:** The direct costs of a breach can be enormous, encompassing the theft of funds, the expense of remediation, regulatory fines, and legal fees.

> **Reputational Damage:** The loss of client trust following a cyberattack can be difficult. This can lead to a mass exodus of clients and a severely tarnished brand.

> **Operational Disruption:** A successful attack, such as a ransomware incident, can bring business operations to a complete standstill, preventing your business from serving its clients, paying suppliers and conducting its business.

	ComplianceSuite
Full Device Encryption	✓
Remote Lock / Kill / Locate	✓
RiskResponders® for Automatic & Off-Network Protections + MFA	✓
Access Controls, USB Port Blocking & M365/Google MFA Analysis	✓
*Secure PDF Email Encryption + Check4Phish™	✓
SendGuard365 Lite for Users to confirm recipients when emailing	✓
Cybersecurity Awareness Training + Dark Web Monitoring	✓
Vulnerability Assessments & Attack Surface Monitoring	✓
Data Protection Compliance Toolkit + ComplianceKate® AI Assistant	✓
ComplianceEZ® for NIST / CIS / ISO27001 CSF Assessment	✓
Managed DMARC & MTA-STS for Email Security Compliance	✓
**R1M Cyber Warranty	✓

Encrypt | **Safeguard** | **Protect** | **Defend**

* COM Addin for Microsoft Classic Outlook on Windows PC. ** Cyber Warranty only applies to SMEs domiciled in South Africa.

SMBsecure™

PROTECT & SECURE PATIENT PERSONAL DATA

Protecting patient information is a professional and legal obligation. Weak security can lead to patient harm, loss of trust, regulatory penalties, and practice disruption.

HPCSA Guidance

Patient information must be treated as confidential. Electronic and telemedicine records must be safeguarded. Security measures should be documented, including encryption, password-protected systems, and controlled access to records.

POPIA Safeguards

Medical practices must implement appropriate technical and organisational measures to protect the integrity and confidentiality of personal information and be prepared to respond to and notify affected parties of data breaches.

Key Controls To Implement Now

- ✓ Role-based access control and unique user accounts.
- ✓ Strong passwords and multi-factor authentication to secure & verify access.
- ✓ Encryption of patient data at rest and in transit, and on portable devices.
- ✓ Secure, encrypted backups tested regularly.
- ✓ Device security: screen locks, updates, antivirus, remote lock/wipe.
- ✓ Email security: DMARC, MTA-STS (TLS).
- ✓ Audit logs and regular review of access to records.
- ✓ Staff training and written data protection policies with documented proof.

Mapping regulatory duties to concrete controls demonstrates reasonableness, a critical factor in defending HPCSA complaints and POPIA investigations.

When Patient Data Goes Wrong
A realistic scenario for doctors in small practices

The Scenario

A staff member's laptop containing unencrypted patient records is stolen from a vehicle. No access controls were in place. The practice has no documented security controls.

What Happens Next

1 Patients complain after data appears online.
2 HPCSA opens an ethics investigation.
3 POPIA requires breach notification and investigation.
4 The doctor must explain why encryption and access controls were not used.

The Uncomfortable Question

"Doctor, what reasonable steps did you take to protect patient information?"

How SMBsecure™ ComplianceSuite Changes The Outcome

Encryption, access controls, audit logs, and documented policies and proof of measures provide defensibility and significantly reduce professional and legal exposure.