SMBsecure™

For Medical Practices

Patient Confidentiality | Data Security | Compliance

Overview of Service

Medical Practices are targets for cyber criminals to obtain personal information. Exposed personal information places patients at risk of financial losses stemming from identity theft, scams, and fraud.

SMBsecure™ is a neat and affordable solution bundle for data protection stipulated by HPCSA, Medical Aids and the POPI Act,

This solution employs necessary security measures and controls to mitigate risks of unauthorised data access and exposure. It is tailored to help medical practices and healthcare practitioners stay secure and earn trust while remaining compliant.

HOW IT WORKS

SMBsecure™ is an All-in-One service to de-risk your medical practice with Data-on-Device Encryption, Device Access Controls, Secure PDF Email Encryption, Device Lock/Kill, Cyber Risk Awareness Education, Reporting and Proof of Data Encryption.

Beyond your consent form, the SMBsecure™ POPI Toolkit is an add-on DIY resource kit to help you comply with the POPI Act.

Securing personal data from unauthorised exposure is a critical HCP & compliance requirement!

COMPLY WITH HPCSA

The Health Professions Council of South Africa (**HPCSA**) prescribes your ethical guidelines and good practice. The right of patients to privacy, security and confidentiality must be protected at all times. Therefore, effective safeguards against unauthorised use and the secure transmission of confidential patient information must be assured. All patient and clinical records stored on computer drives are to be encrypted and access to the device is controlled by a password to prevent unauthorised access to this information (**patient personal data**).

The HPCSA stipulates that any electronic transmissions which include patient personal data (e.g. emails, prescriptions, and laboratory results) must be secured. It is the responsibility of healthcare practitioners to ensure that non-healthcare personnel do not violate patient confidentiality. When it comes to the processing of patient information, the HPCSA states that a healthcare practitioner (**HCP**):

1. **Must** be satisfied that there are appropriate arrangements for the security of personal information when it is stored, sent or received by computer, e-mail or other electronic means.
2. **Must** make sure that their own computer terminals or any other communication devices are secure at all times. If they send data by email or any electronic format, they should satisfy themselves, as far as is practicable, that the data cannot be intercepted or seen by anyone other than the intended recipient. Healthcare practitioners should note that information sent through the Internet may be intercepted.
3. **Should** include details of the security measures taken such as data encryption and authentication controls with the informed consent documentation for telemedicine practice.

MEDICAL AIDS AND POPIA REQUIREMENTS FOR HEALTHCARE

Both the POPI Act (**POPIA**) and Medical Aid administrators demand proper safeguards of patient personal data.

Where an email is being sent with files which contain or include personal information (patient personal data), it must be password encrypted. A practice must ensure that any communication with patient personal information sent to a medical aid administrator is sent securely.

Necessary security measures must be in-place - *with proof* - on your computers and mobile devices to mitigate unauthorised access and data exposure. Ensure that if a device is stolen it can be locked or killed, removing all access to the perpetrator. These protections must also apply to your operators (e.g. debt collectors).

Sources: https://www.hpcsa.co.za/ | https://www.discovery.co.za
https://smbsecure.co.za/popia/