The Protection of Personal Information Act 3 of 2013 (POPI) will become effective in the course of 2015. This Act places an extra responsibility on doctors to monitor and self-report their own flow of personal information to help protect patient privacy.

POPI affects all healthcare service providers in the private and public sector that process (collect, keep and share) personal information such as names, addresses, email addresses, health information and employment history.

It does not replace the HPCSA’s existing guidance Confidentiality: Protecting and Providing Information, on safeguarding confidential patient data.

In terms of the HPCSA’s guidelines, a healthcare practitioner may make records available to another healthcare practitioner without the consent of the patient if such other practitioner requires the records to defend a claim for damages or defend charges of misconduct (see HPCSA booklet 14 paragraph 11.2). When the protection of Personal Information Act becomes effective it would be advisable to contact MPS before a disclosure is made in terms of these regulatory guidelines. In so far as the HPCSA guidelines set out above may be in conflict with the provisions of POPI, the provisions of the Act will prevail.

Collecting personal information

Under POPI, personal information may only be collected for the specific purpose of providing services to a particular subject (ie, patient). If another doctor provides you with a patient’s personal information, it will only be in the patient’s legitimate interests for you to hold this information if you are providing your services to that patient.

Once personal information has been collected from another source, the medical practitioner must take reasonable steps to inform the patient of this, together with the source of the information and the purpose for which it has been collected. This can be relayed to the patient either orally or in writing.

Preserving personal information

Any personal information you hold must be protected from loss, damage or unauthorised destruction, and unlawful access. You should implement reasonable technical and organisational measures to ensure this. However, the resources of your organisation will be taken into account, as well as the nature of the information, when determining reasonable measures.

As a minimum, doctors are expected to identify all reasonable foreseeable internal and external risks, establish appropriate safeguards, and regularly review these. MPS recommends you carry out a risk assessment and draw up a protocol. Examples of foreseeable risks are:

- **Access to information**
  - Employees requiring access to patient information should be identified and should have employment agreements that include a clause to keep information strictly confidential.
  - Employees should have individual passwords to access patient information, which are updated from time to time. A generic password for all staff is not acceptable.

- **Accidental destruction**
  - Hard drive or server crashes can destroy personal information. Ensure suitable back-up is in place to either limit or prevent this.

- **Theft**
  - Ensure hard copies of patient information are stored securely in locked filing cabinets or rooms. Patient files should never be left unattended.

Third party access

Under the terms of POPI, the arrangements around third party access to patient information broadly match the guidelines set out by the HPCSA. Patient consent is needed in most situations but is not necessary in others.
If, for example, an IT service provider is installing new software in your practice or hospital, the rules of POPI mean that they may only process personal information if the responsible party is aware of it, and as long as the operator has agreed to treat all personal information they encounter as confidential. The operator must also notify the responsible party if any information is leaked to an unauthorised party – it is recommended that all this is agreed in writing.

**Information leak**

Any suspicion (on reasonable grounds) that personal information has been accessed or acquired by an unauthorised person must be reported to both the patient and the Information Regulator. Notification must be in writing and must provide sufficient information to allow the patient to understand:

- The possible consequences of the unauthorised disclosure for him/her
- A description of the measures that you intend to take to protect his/her interests
- The identity of the individual who made the unauthorised access.

and decide whether s/he would like to take any protective steps.

**Failing to comply with POPI**

Failure to comply with the provisions of POPI can potentially lead to:

- A complaint lodged with the Information Regulator
- Receiving a civil claim for payment of any damages
- Criminal prosecution – if convicted there could be a fine up to R10 million or a prison sentence up to ten years, or even both.

If you are unsure of your new obligations, or are preparing to report a possible breach of personal information to the Information Regulator and a patient and would like further advice, please contact MPS.

**Further information:**

- HPCSA, Confidentiality: Protecting and Providing Information – [www.hpcsa.co.za](http://www.hpcsa.co.za)

For medicolegal advice please call us on:
0800 982 766 (toll free)
or email us at:
medical.rsa@mps-group.org
www.mps-group.org

This factsheet provides only a general overview of the topic and should not be relied upon as definitive guidance. If you are an MPS member, and you are facing an ethical or legal dilemma, call and ask to speak to a medicolegal adviser, who will give you specific advice.

MPS is not an insurance company. All the benefits of membership of MPS are discretionary as set out in the Memorandum and Articles of Association. The Medical Protection Society Limited. A company limited by guarantee. Registered in England No. 36142 at 33 Cavendish Square, London, W1G OPS.