FACT SHEET FOR MEDICAL PROFESSIONALS

Handling patient information under POPIA

The Protection of Personal Information Act, 2013 (POPIA) imposes minimum standards on the way personal information is collected, stored, used, disclosed, and deleted. The healthcare sector handles some of the most sensitive information including physical and mental health records of patients.

Medical practitioners also have obligations in handling personal information under under the National Health Act, 2003 and the guidelines issued by the Health Professions Council of South Africa under the Health Professions Act, 1974.

This fact sheet sets out practical guidelines to assist medical practitioner comply with their obligations under POPIA and should be read with the Guidance Note for POPIA Compliance by Institutions and Individual Practitioner Healthcare Providers attached to this fact sheet.

Collection of information

- Only collect Information that you need for a specific purpose (i.e. treating patients).
- Ensure that the patient is aware of the purpose for which the information is collected and who the information will be shared with.
- Ensure that there are notices in areas where CCTV cameras are used.

Destruction and deletion of information

- If you are no longer authorised to keep the personal information contained in health records, ensure that it is disposed of securely.
- Physical records could be shredded, pulped, or burned.
- Electronic records could be deleted, meaning that a person without special technical IT skills would not be able to access or re-create the deleted records.
- If practical, electronic records should be destroyed by formatting the hard drive or using software to overwrite the records.

Storage of information

- Keep both physical and electronic information secure.
- Control access to physical files through access cards and locking files in a secure filing cabinet or vault.
- Ensure electronic information is secure with password protection, up to date antivirus software and firewalls. USBs, mobile phones, and computer connections used to transfer information or store health records should be secure (for example, use encrypted USBs or allow access to records only through secure mobile applications). You must train staff in the proper handling of health records.

Sharing of information

- All information relating to a patient's health and treatment is confidential. You must have the informed consent of your patient to disclose this information to another person except where you seek the specialist advice of another medical professional during treatment or in corresponding with a medical scheme regarding payment. If your patient is a child, you would need the consent of the child's parent or legal guardian.
- Ensure that contracts with service providers such as waste disposal companies, laboratories or IT service providers include POPI compliant clauses.

Retention of information

- Ensure that the information is relevant and up to date.
- Have a records policy that sets criteria for keeping information, or where appropriate, the specific
- retention periods for certain categories of information.

Requests for access to information

- Your patients have rights to see their personal information.
- You must allow a patient to see their information on receipt of a valid request in the manner prescribed in your privacy policy if there are no lawful reasons to refuse access.
- Patients can require that their personal information be corrected or deleted.
- You may refuse to do so where the information is your professional opinion, but you must make a note of the challenge on the relevant record.

itoo.co.za

@itooexpert

011 351 5000