Information management and healthcare.

Nina Kriel
BOptom, BSc Hons, BA Hons, OD, LLB.

Issue 2 (2015):
The Protection of Personal Information Act
ODO001/007/05/2014
Background

The patient’s right to privacy in the sphere of healthcare has recently been brought under the spotlight by several unrelated, but contributing developments:

1. The USA is the process of implementing electronic health record (EHR) systems in an effort to curb spiralling healthcare costs.
2. The Protection of Personal Information Act was signed into law by the president of South Africa, and gazetted in November 2013.
3. Internet & communication technology (ICT) facilitates and encourages sharing of a great deal of personal information. What are the implications for privacy, particularly in healthcare?
4. Patients and practitioners are bombarded with too much information, yet struggle to access pertinent, accurate and reliable information.

Privacy and safety

Meet the fictitious Mrs Rattanakosin (aged 78) who lives in Thailand and was visiting her son in South Africa when she presented to you on a Monday morning complaining of pain in the second quadrant and left ear. She doesn’t speak much English but, she is a member of HealthWeb, an advanced electronic health record (EHR) management system, which her son though may be of assistance. Having down-loaded the HealthWeb app on your smartphone, Mrs R needed only to place her finger on your smartphone screen, confirming her identity by fingerprint, to give you access to her EHRs. ‘Aided’ by the HealthWeb system, we took an inordinate amount of time to complete an examination on Mrs R, almost being led astray by the sheer volume of information presented. Could we have used the information better?

Not only could we have done a better job, but we will soon be legally obliged to manage patients’ information better. The president signed the Protection of Personal Information (POPI) Act in November 2013. The Act has not commenced in its entirety, but as of 11 April 2014 the definitions apply and the regulator is being formed which will compel us to do better by patients like Mrs R in future.
What does the POPI Act hope to achieve?

Our Constitution recognises several basic human rights, including privacy. The Constitution does not go into much detail, so several subsequent pieces of legislation have been created to flesh out the bare bones provided by the Constitution. The purpose of the POPI Act is to (s2):

(a) give effect to the constitutional right to privacy, by safeguarding personal information when processed by a responsible party, subject to justifiable limitations that are aimed at—

(i) balancing the right to privacy against other rights, particularly the right of access to information; and...

(b) regulate the manner in which personal information may be processed, by establishing conditions, in harmony with international standards, that prescribe the minimum threshold requirements for the lawful processing of personal information;

(c) provide persons with rights and remedies to protect their personal information from processing that is not in accordance with this Act; and

(d) establish voluntary and compulsory measures, including the establishment of an Information Regulator, to ensure respect for and to promote, enforce and fulfil the rights protected by this Act.

Don’t be alarmed by all of that. It simply means that the purpose of the Act is to specify who can handle your information and how; that they must balance your rights to privacy with your right to information while considering the rights of others too. It creates a set of rules (based on international standards) for us and creates a watchdog to ensure we follow those rules. The Act is actually quite straightforward. To ensure everyone’s on the same page, legislation typically includes definitions of key concepts. Section 1 includes these:

Personal information is information that relates to an identifiable, living, natural person or an identifiable, existing juristic person. This means that a practice, for example, as a juristic person is also protected by the Act. Information relating to the race, gender, sex, pregnancy, marital status, nationality, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person; their education or the medical, financial, criminal or employment history and any identifying number, symbol, e-mail address, physical address, telephone number,
location information, online identifier or other particular assignment to the person. Also, any biometric information of the person, (we’ll get to the definition of ‘biometric’ in the Act) and even the personal opinions, views or preferences of the person or of someone else about that person. That means that your opinion (e.g. a diagnosis or report) of a patient is considered personal information. Any correspondence sent by the person that is implicitly or explicitly of a private or confidential nature, including any attachments or messages included in forwarded mails are all included.

By now I’m sure it’s clear that almost every piece of information that the patient gives us, or that we discover during examination meets the definition of ‘personal information’ and the Act applies.

**Processing** means any operation/activity/set of operations, whether or not by automatic means, concerning personal information, including the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; dissemination by means of transmission, distribution or making available in any other form; or merging, linking, restriction, degradation, erasure or destruction of information. Again, we certainly process information, and it’s important to note that even destroying information is considered processing and is covered by the Act.

**Record** means any recorded information regardless of form or medium, including writing on any material, information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored... book, map, plan, graph or drawing, photograph, film, negative, tape or other device in which one or more visual images are embodied...in the possession or under the control of a responsible party; whether the responsible party created it or not.

The **responsible party** is the private or public party who determines the purpose and means of the information processing. In most cases, this is the practice owner/dentist, but in certain circumstances it may include the software company, the franchisor or other administrative provider. (There is a technical difference between a responsible party & an operator, which I won’t get into here.)
The **data subject** is the person to whom the information refers, in our case usually the patient, although we will also process personal information of the person responsible for payment (e.g. a parent, employer or a medical aid) as well as personal information about our staff and even our suppliers.

Clearly it’s necessary to process personal information to continue a healthcare practice, so how do we comply? The POPI Act was 8 years in the making, mostly to ensure that we comply with international privacy standards. Foreign legislation refers to privacy ‘principles’ (EU) and POPI refers to ‘conditions’ for the legal processing of personal information. There are 8:

- Accountability
- Processing limitation
- Purpose specification
- Further processing limitation
- Information quality
- Openness
- Security safeguards
- Data subject participation

I’ll explain each one and also give tips on making your practice compliant.

**Condition 1: Accountability**

The responsible party has to ensure compliance with these 8 conditions for lawful processing. The responsible party is defined by the Act ([see p 4 of this article](#) for a review) but is most likely the practice owner, not the staff or 3rd parties processing the information on their behalf. It is still important to recognise the roll we play.

**To do:**

- Explain to the dental team that just about all the information that they deal with is now regulated by law. Explain that besides the penalties, it is good practice to maintain privacy anyway.
- Staff should never discuss patients where others can hear, either inside the practice or outside.
- Patient records should not lie around where other patients can see them.
If you verbally collect/update patients’ information, give them the opportunity to do so in private. Privacy is one of the arguments in favour of a paper system of collecting personal information. A tablet based system is not going to work for everybody. Remember when our fictitious patient Mrs R came in to the practice and we set her up to complete the questionnaire in the privacy of the accounts section? Can we assume that an older lady in a strange environment can confidently and accurately answer healthcare questions? Even if Health-Web translates, will the translations be accurate? The Asian languages are notoriously (and sometimes amusingly) difficult to translate, but if healthcare information were to get lost in translation, it would be no joke!

**Condition 2: Processing limitation**

Collection of certain personal information from a patient is justified, but the information that we gather should not unreasonably infringe on any rights of the patient. Aim to collect the minimum, but adequate information required for the objectives. The patient should consent to you gathering the information. Consent is a ‘voluntary, specific and informed expression of will’ (s1) so a 3rd party cannot give consent to process information unless they are the parent or guardian of a minor or incompetent patient. Gathering information from the data subject (patient) him/herself ensures that the patient knows and consents to the information that you have.

**To do:**

- There’s a fine line between collecting the minimum information and not having enough to ensure good care or to carry out the contract to provide care. What is relevant depends on the situation. We would not gather the same information from an out-of-town patient having their denture repaired while on holiday as we would from a diabetic patient with an abscess. Use a few examples like these to explain and set policies for the practice on what data is required.
Patients must consent to the processing of their information and, if necessary, the onus will be on you as the responsible party to prove that you did have consent. Collecting your patients’ personal information on paper is not required, but it does make it easier if patients write it down for you. Both the Companies Act and King III put the responsibility for obtaining consent on management, which again, is probably the dentist/ practice owner.

Patients have a right to know what information we have on them. If Mr X’s biteplate has been ready for weeks and his cell is constantly on voicemail, can you phone his GP to check whether they have an alternative number for him? Strictly, no, although you could argue that it is in his interest to get his biteplate to give relief from TMD symptoms, especially if he has already paid for it. If the shoe were on the other foot and the GP phoned you requesting Mr X’s number, would you give out his telephone numbers? Would it make a difference to you whether the GP is looking for him about his account or to discuss critical lab results? POPI makes provision for exceptions ‘to protect or pursue a legitimate interest.’ We don’t yet know what constitutes a legitimate interest. If Mr X’s information is in the public domain (e.g. in the phone directory, his business website or his WhatsApp status) it is not protected in terms of the Act.

Condition 3: Purpose specification

When we process a patient’s data, the specific purpose is to provide healthcare. Should we decide to start selling cell phones or cupcakes as an alternative income stream, we may not use that information for the (new) purpose of marketing these services. You are obliged to restrict the processing of information to the purpose for which it was first gathered.

Purpose specification also impacts on how, and how long we retain personal information. Again, the balance is to keep it long enough to provide the right care, but not for an unnecessarily long time. Can a cell phone provider kept information on a subscriber even after he had cancelled his contract and had paid all outstanding balances. Not only does this infringe on his privacy, but having his information out there leaves him at risk should hackers breach the cell phone company’s security. If the patient’s history is no longer relevant, destroy the records.
To do:

- We should understand and be able to tell patients why the information is being collected.
- We should know how long records have to be kept. The Health Professions Council requires us to keep records for 6 years, but if the patient’s condition is an ongoing/ degenerative one (e.g. periodontitis) or one where the history is vital (e.g. implant information), it may have to be kept up to 25 years. Because there is legal prescription does not run against minors, pediatric records should be kept until the patient is 21.
- Once you have identified the records to be destroyed, you can’t simply leave them in a black bag on the pavement on a Tuesday morning. There are paper companies that will collect, shred and then recycle your confidential records.

**Condition 4: Further processing limitation**

Closely related to the previous condition, further processing of information is most likely to occur in our case when we conduct research on our existing database.

**Example:** A pharmaceutical company wants to access your records to compare your prescribing habits for pain medications to another practice in the same suburb. This would not be allowed, but it doesn’t mean we’ll never see any clinical research again. The information must simply be de-identified. Instead of saying you prescribed product X for Mrs A, Ms B and Mr C and product Y for Mrs D, you may say that that you prescribed product X 3 out of 4 times, or even that you prescribed product X for 2 out of 3 women. There should be no way to re-identify the patients so ID numbers or account numbers cannot be used.

Further processing must be related to the original reason for gathering information.

**Condition 5: Information quality**

Without complete and accurate clinical information, we cannot make a diagnosis or decide on a treatment plan. Similarly, we need to ensure that the administrative information we have enables us to achieve our purpose. Safeguard all the personal information you hold by keeping it complete, accurate and current/updated. Incomplete information is potentially misleading.
Condition 6: Openness

In the interest of fairness and transparency, data subjects should know what data is being held about them and for what purpose, whether they give it voluntarily or are required to do so by law and whether information will be gathered about them from some other source. Mrs R, for example, by giving us her fingerprint, allows us to gather medical information about her from her electronic healthcare record system, HealthWeb. It sounds like Mrs R may not have been aware that HealthWeb has also accessed her genetic information from 23andMe. (23andMe is a privately held personal genomics and biotechnology company based in California)

Data subjects should have access to information about any entity that processes their personal information. Your practice information should be accessible to patients both in terms of the Promotion of Access to Information Act (PAIA) as well as the POPI Act.

Personal information may not be processed without notifying the data subject unless their data has been rendered non-identifiable or it is the public interest to do so.

Condition 7: Security safeguards

Apply Generally Accepted Information Security Principles (GAISP) to protect the integrity and confidentiality of personal information. Both physical and digital data should be secured and protected. Where there is a breach, both the information regulator and the data subject must be notified.

To do:

- Protect the physical security of your patient records by keeping filing up to date. Cards piling up on desks create the opportunity for others to gain access to information.
- US legislation requires electronic health records to be encrypted. POPI is not as strict, but password protection is highly recommended.
- Staff must be told at employment, and reminded thereafter, that all information that they have access to is confidential. Protecting the integrity and security of information is required by law.
Condition 8: Data subject participation

In terms of POPI, patients must be able to check whether (for free) and what (at 'not unreasonable cost') information is being held about them. A data subject may request correction or deletion of his/her data held by the responsible party.

To do:

Ensure that staff know that patients may request this information. Responding to such requests should be done accurately and consistently, considering that they may be the prelude to a legal challenge.

Direct marketing

Chapter 8 of the POPI Act is dedicated to the rights of data subjects regarding direct marketing by means of unsolicited electronic communications, directories and automated decision making.

Most of us communicate with our database (patients) regularly. We update them on services the practice offers, promotions and new products. POPI regulates such communication, whether by SMS, fax or e-mail.

You may only market to actual patients. If you have sponsored a golf day and the golf club has given you access to the list of players, you may not market to them because you did not get their contact details ‘in the context of the sale of a product or service.’ (s69(3)(a)) As I mentioned before, you are restricted to marketing your own ‘similar products or services’ and not your budding cupcake or cell phone business. Even with these restrictions, patients must be given reasonable opportunity to opt out, at no cost to them and without undue formality. Patients must be able to opt out at the time that you first gather their information and each time that you communicate with them.

A data subject may consent to receiving information from you, whether they are a patient or not, and of course then you may market to your heart’s content.
To do:

- Include tick boxes on the patient forms so the patients can opt in or out.
- Encourage opt-ins by specifying how often and what you will communicate.

Use a little psychology when designing your forms. People don’t read, and they are more likely to leave boxes blank than ticked. Phrase your question so that a blank box means you may communicate with them. Here are some examples:

- We would like to keep you informed of products and services that we offer. Please tick here if you would not like to receive an e-mail from us twice a year.

- We would like to send you an SMS to remind you when you are due for your next dental examination. Tick here if you prefer not to receive reminders.

If the patient does tick the boxes you can confirm verbally: ‘I see you have opted not to receive news of the latest developments or products that may be useful to you. Is that correct?’ You may update their preferences at each visit or check up, but you may not request consent over and over again until you wear them down. Using our earlier example of the list of golfers from the day your practice sponsored at the club: Once they have refused consent, you may not approach them again. Consent may be withdrawn by the data subject at any time.

The future of personal information processing?

The Act has not yet fully commenced and we do not (at present) have a commencement date. When it does, we will have 1 year to become compliant. It’s important to start becoming compliant now. Once the Act commences it will be further developed in several ways:

- Cases which will show us how the regulator and the courts interpret and apply the Act.
- Codes of conduct are provided for in the Act. They may not be less restrictive
than the Act and they must include all 8 conditions for the legal processing of personal information (or a functional equivalent.) The purpose of a code of conduct is to give responsible parties in a particular sector (e.g. the healthcare sector) clearer guidance on processing personal information. The Code of Conduct can be developed by any interest group, a professional association or another regulator. The HPCSA may, for example, approach the information regulator with a Code of Conduct, or may publish a code of conduct. The information regulator may revoke a Code of Conduct.

- Settlements are to be gazetted. Besides the cost of a punitive or administrative fine, transgressors will be exposed to bad press. Imagine the damage to your practice’s reputation! It’s not worth risking.
- Children’s rights: POPI adopts the UN definition of a child i.e. a person under 18 years of age. A child must be assisted by a competent person to consent to the processing of his/her personal information (s11) and a competent person may give personal information on behalf of a child (s12). This is an exception to condition 2 which requires us to gather information directly from the data subject. However, in conflict with this is the Children’s Act which allows children to consent independently from the age of 12, if ‘the child is of sufficient maturity and has the mental capacity to understand the benefits, risks, social and other implications of the treatment.’ For surgery, the child has to be assisted by a parent or guardian, but they do not need to consent on behalf of the child. Children may open bank accounts unassisted from the age of 16. How are banks and healthcare providers to comply with a child’s legal wishes to be treated, or open an account when they may not legally consent to processing of their information? In keeping with current practices of involving patients with their healthcare decisions, experts anticipate that updates to POPI will review this age downward. Foreign legislation also supports a younger age of consent for personal information processing. The US’s Children’s Online Privacy Protection Act (COPPA) was crafted to protect children’s privacy and safety online and prohibits marketing to children under 13 years of age.
Protecting Personal Information in Electronic Health Records (EHRs)

A national centralised EHR system is being rolled out in the US with the intention of reaching ‘meaningful use,’ originally by October 2014, but the implementation deadline has been pushed back (again.) Meaningful use requires the complete transition to EHR and is aimed at improving clinical outcomes and protecting patients’ rights by increasing their engagement in healthcare decisions. Participation by the US private sector is not compulsory, but payment is higher for practitioners who do achieve meaningful use. The difference over 10 years could be $63 000 according to the [Centres for Medicare and Medicaid](https://www.cms.gov), but several professional and hospital organisations have declared the timeline too aggressive and have all but given up.

If the US is experiencing resistance and teething problems, can we ever expect EHRs to be implemented here? Do we want them, considering that they seem to increase our risk for privacy infringements? Internet access is prohibitively expensive and mind-numbingly slow here so our lives are not as ‘online’ as the rest of the world but before you dismiss the concept entirely, consider these facts:

- The online retail sector in SA exceeds **R2 billion** and is growing by 30% per year.
- Annual online airline ticket sales in SA are estimated to be **over R10 billion**. Who still uses a travel agent? Brilliant websites and innovative approaches to travel (e.g. home exchanges, airbnb’s and couchsurfing) have spelled doom for traditional travel agents. Only niche and bespoke operators, and discounters at the other end of the spectrum, seem to have weathered the storm. Our profession can learn from this.
- **About 80%** of South Africans with internet access do shop online. More than 32 million adults (age 15 and above) use a cell phone. At present only 40% of those are smart phones but expansion will push online retail, and with that the online presence of each one of us. How will that affect dental care?
- Medical aids are positive about EHRs. Medical aids want to keep patients happy and well at the minimum cost. That’s good for their shareholders in the end.
There’s no denying that EHRs, correctly used, can save costs and improve patient outcomes, but besides that benefit, we are in the unusual position of being the perfect testing ground for developers of EHRs for the US market. The US is still using ICD9, and should make the move to ICD10 in 2015, although they keep postponing that date. One local medical aid is even handing out iPads to general medicine practices to encourage practitioners to participate in the testing. International players like Meditech already have a local footprint in SA, so it’s safe to assume that we will be influenced by the trend towards digital healthcare.

What are the drivers for the move to EHR?

I’ve mentioned the potential financial and clinical benefits of EHRs, but another crucial aspect of health care in the US is avoiding litigation. For that reason, if a patient’s data is not readily available from a trusted source, the test is duplicated. If we want to know a patient’s blood type, we could ask the patient or their family, or check their previous provider’s records, but rather than accepting such critical information second hand, or from a source we can’t trust, the test is repeated because it’s quick, inexpensive and conclusive. It’s not worth risking a mistake. What if the test cost thousands of rands? Or if the procedure itself carried some risk? Patients need to give informed consent for every healthcare intervention, from surgery to the electric toothbrush that we recommend for them. But explaining a procedure with all its risks and benefits is an important, but onerous and time consuming process.

More admin means more staff and higher healthcare costs. With EHRs we could easily check the patient’s history & mitigate risks appropriately.

EHR systems can be used to educate the patient. Because internet penetration is high in the US (79%) the chances are that most American patients are comfortable with computers. A computer, or even internet-based system could well provide the information necessary for informed consent without tying up a staff member. Internet penetration in Africa is much lower: South Africa is at 17.4%, Botswana at 12.8% and Namibia at 12%. (The world average is 34.3%)
Can we assume that patients here are as comfortable with IT? Even if they know how to use a tablet, do they have the dexterity to tick the correct boxes?

The gentleman in the video below has come up with an ingenious application for this modern marvel.

I’ve mentioned that our insurers and medical aids’ focus is forensic; avoiding fraud and over-servicing, but the needs of government are similar – serving as many people as possible with limited human and financial resources – so the appeal is obvious. The added benefits of administrative management and built-in reporting are just a bonus.

I have looked at several appealing record management systems in use in the US, but so far no one system ticks all the boxes, and they’re expensive. Patient care with insufficient information is difficult, but with too much information it can be equally challenging. In fact, substantial EHR and risk management programme led us astray. With too much information, EHR systems, particularly those developed for the US, aim to protect the practitioner or the facility against litigation, not help us make clinical decisions. EHR systems will flag the most likely causes of a legal action, not the most likely clinical causes of implant failure. We still need to apply our minds to find the correct diagnosis and formulate a treatment
plan. What if my differential diagnosis or treatment plan differs from that proposed by the system? We all aim to practice in a manner that is supported by evidence, yet treatment approaches differ.

- Is your approach current?
- Is the EHR’s recommendation based on current research?

Research can be expensive to access and difficult to interpret.

According to the computer, I need to back up your kidneys, defragment your liver and reboot your heart.'

Cell phone ≠ internet

Because of our poor IT infrastructure, the fastest growth in internet access is via cell phone. Although approximately 32 million adults in South Africa own or have use of a cell phone, it would be inaccurate to infer similar internet access. Many of these phones are not smart phones. Less than half of ROOTS 2013 respondents had a smart phone. Of all cell phones in use in SA, 56% are Nokia, 17% Samsung & 13% BlackBerry. Just 1% are Apple iPhones.

Understanding patients

As patients’ needs and interests change, so do their media choices. Match your information to the patient’s age and demographic.

- The average seventeen magazine reader is 23.
- The average age of Hustler readers is 33. What a difference a decade makes!
- The average SA Home Owner reader is 43.
Questions.

To answer these true/ false questions online, please go to www.synapse.org.za and login, using your email address and registration number. You will need 70% or more to qualify for your 4 ethics CPD points.

1. The Protection of Personal Information Act becomes effective in April 2016.
2. The purpose of the POPI Act is to give effect to the constitutionally protected right to privacy by safeguarding personal information and imposing justifiable limitations.
3. Personal information (as defined by the POPI Act) relates only to personal preferences such as sexual orientation, political affiliations and religious ideology so are unlikely to impact on healthcare.
4. Processing is the act of altering data for research purposes to ensure that the subjects cannot be individually identified afterward.
5. The term ‘data subject’ is the person to whom the information refers. In the case of information processing in an dental practice, our data subjects are only patients.
6. The principle of processing limitation allows us to collect personal information from a patient provided it is justified and does not unreasonably infringe on their rights.

The future of casts?

Some of you may know first hand the woes of wearing a cast. It’s itchy, smelly, heavy... This prototype, called the Osteoid, was made using a 3D printer and, by using the built-in low-intensity ultrasound system for only 20 minutes a day, the healing process can be up to 40% faster.
Consent is a voluntary, specific and informed expression of will.

The HPCSA requires written informed consent for treatment by any of its members.

Personal information collected by dentists may be shared with other healthcare providers without obtaining the patient’s consent.

Samuel is 17 and has an implant. You should keep his records until his 21st birthday.

The POPI Act requires us to keep patients’ personal information accurate, current/updated and complete.

The openness condition protects the patient by encouraging healthcare providers to make clinical information accessible (open) to the patient’s treating doctors and contracted medical aid.

POPI does not require electronic health records to be encrypted but password protection of digital healthcare information is highly recommended.

Patients should be able to access information held about them, but can be charged a reasonable fee e.g. when a written report is required.

Smiles-R-Us notify their current patients by SMS that they will receive weekly notice of specials but, should they wish to, they can opt out by return SMS. The cost of the SMS is R10.00. This Smiles-R-Us campaign is POPI compliant.

POPI compliance will be mandatory from 1 year after the commencement date of those sections of the Act.

The Children’s Act allows children to consent to healthcare independently from the age of 12, provided the child is mature enough to understand the benefits, risks and other consequences of such treatment.

About 80% of South Africans have smart phones.

Medical Aids are in favour of the use of electronic health record systems.

South Africa will start implementing ICD10 codes in July 2015.