INFO on Healthcare industry

POPIA and the Healthcare industry

Source: https://www.michalsons.com/blog/privacy-in-healthcare/8637

The most important laws that relate to data protection in healthcare

1. Constitution
2. Common law obligation of confidentiality
3. The Promotion of Access to Information Act (PAIA) – for example, a requester might be able to request access to the HIV status of another person
4. Various medical laws or codes relevant to patient information (like the National Health Act, HPCSA Ethical guidelines for good practice in the health care professions and the Ethical Charter,specifically Rule 2.3.8, Rule 5.4 and Rule 13 respectively. See also Confidentiality: Protecting and Providing Information)
5. The POPI Act or POPIA

These are not all of the laws, just some of the more important ones. It is important to look at all relevant laws when considering the application of them to issues. In this article, we are just going to look at two laws and how they interact. You can also read more about information security legal requirements in different healthcare laws.

Which law prevails?

Whichever provides the patient with greater protection or rights (the more extensive provisions) prevail. So often this means that healthcare law (like the National Healthcare Act) prevails over data protection law (POPIA). For this reason, it is very important to create a matrix of all applicable laws to help you work out which one prevails in a particular case.

National Health Act (NHA)

A patient's information is confidential and a person may only disclose it in certain circumstances

All information concerning a user (including information relating to his or her health status, treatment or stay in a health establishment) is **confidential** (section 14). **No person may disclose** any information unless:

- the user **consents** to that disclosure in writing;
- a **court order** or any law (like PAIA or section 15 of the NHA) requires that disclosure; **or**
- non-disclosure of the information represents a **serious threat to public health**.

A health worker may disclose for a legitimate purpose in the interests of a patient

"A health worker … that has access to the **health records** of a user **may disclose** such personal information to any other person, health care provider or health establishment as is necessary for any **legitimate purpose** within the **ordinary course and scope** of his or her duties where such access or disclosure is in **the interests of the user**." (section 15)

A healthcare provider may access health records

A health care provider may examine a user's health records for the purposes of:

- treatment with the authorisation of the user; and
- study, teaching or research with the authorisation of the user, head of the health establishment concerned
  and the relevant health research ethics committee (section 16).

A health establishment must protect health records

The person in charge of a health establishment in possession of a user's health records must set up **control measures to prevent unauthorised access** to those records and to the storage facility in which they keep those records (section 17). It also says that anyone who fails to do so commits an offence and is

liable on conviction to a fine or to imprisonment for a period not exceeding one year or to both a fine and imprisonment. The person in charge of a health establishment, such as a hospital or doctor's practice, therefore requires information security to prevent unauthorised access to a user's health records.

Stem cell data is confidential

Section 10 of regulation R183 of the National Health Act says that an authorised stem cell bank must ensure that all data (including genetic information, collated within the scope of this regulation) remain confidential at all times, including ensuring that:

- data security measures are in place as well as safeguards against any unauthorised data additions, deletions or modifications to donor files or deferral records and transfer of information;
- procedures are in place to resolve data discrepancies;
- no unauthorised disclosure of information occurs, whilst guaranteeing the traceability of donations; and
- anonymity and privacy of donors are protected.

The POPI Act and healthcare

The definition of personal information includes:

- "information relating to the … physical or mental health, well-being, disability … of the person", and
- "information relating to the … medical … history of the person".

Special personal information includes "*information concerning the … health … of a data subject*". A person's current coronavirus status is definitely special personal information. Sometime after that, it might become the medical history of the person and therefore only personal information.

There is an interesting distinction here. **Medical history** is about the past whereas **health** is about the present. Therefore, different rules apply to those two different kinds of personal information. Seems strange and could result in some interesting practical applications. When it comes to a person's medical history the normal conditions under Part A of POPIA apply. But when it comes to health the authorisations for special personal information apply. Section 26 of POPI prohibits the processing of personal information concerning a person's health. But then (under section 32(1)) the prohibition does not apply to the processing by various people or institutions. Such as:

- medical professionals, healthcare institutions or facilities or social services,
- insurance companies, medical aid scheme administrators and managed healthcare organisations,
- schools, and
- any public or private body managing the care of a child

But that is not the end of the story. Many people will stop reading there and think that they have Carte Blanche. That is not the case. There are conditions and rules that need to be followed in each case. You need to read section 32 carefully. Section 32 also confirms the common law duty of confidentiality or creates it where it does not exist.

Protecting personal information: Implications of the Protection of Personal Information (POPI) Act for healthcare professionals

M Buys

MB ChB, DA (SA), MMed (Anaes), FCA (SA); Specialist anaesthetist, private practice, Western Cape, South Africa

Correspondence

ABSTRACT

Careless handling of patient information in daily medical practice can result in Health Professions Council of South Africa sanction, breach of privacy lawsuits and, in extreme cases, serious monetary penalty or even imprisonment. This review will focus on the Protection of Personal Information (POPI) Act (No. 4 of 2013) and the implications thereof for healthcare professionals in daily practice. Recommendations regarding the safeguarding of information are made.

Although promulgated in November 2013, the Protection of Personal Information (POPI) Act (No. 4 of 2013)[1] still awaits enactment, although sections of the act are already active, dealing mainly with the appointment of the Information Regulator, which was made in December 2016 and formally introduced in February 2017.[2] Following the proclamation of enactment by the President of the Republic of South Africa (the exact date of which is still unsure), individuals and organisations will have a year's grace period to implement the necessary safeguarding measures before the Information Regulator will implement fines and initiate prosecutions.

The main purpose of the POPI act is to protect the processing of personal information by public and private bodies. Balancing the right to privacy against the reasonable right to access of information is paramount in an era that supports both free access to information and personal exposure on social media and digital platforms. The act bears importance for every South African, as it protects the distribution and prevents the abuse of personal information by individuals and corporations, domestically as well as internationally.

Intentional and unintentional exploitation of information

Personal information can be exploited intentionally and unintentionally. Intentional publication of personal information in the healthcare setting is both unethical and illegal,[1,3] as it directly contravenes patient confidentiality. Medical professionals and healthcare institutions have an obligation to maintain confidentiality by virtue of their profession,[1] and the consequences of transgressions can be severe. A clinical example would be mentioning a patient or showing a photograph of a patient publicly (for instance, on social media or other public communication platforms). The roles and implications of social media in the healthcare profession are unfortunately still unappreciated, as is evident by a recent example of a nurse practitioner who mentioned a high-profile politician's family member in her Facebook update, thereby revealing her medical treatment.[4] This led to the employee's immediate dismissal, and necessitated a formal apology to the patient and her family. The interested reader is referred to an excellent recent review of the ethical implications of social media in the healthcare profession.[5]

This article rather aims to focus on the unintentional publication of patient information, which is a more subtle entity, but can carry equally severe consequences. All healthcare professionals and administrative staff acquire personal information on a daily basis. Merely by opening an account or divulging a medical history, a patient provides healthcare professionals with confidential personal information. Legally, this information is regarded as a patient's personal 'property, which is divulged for a specific purpose, in the tacit understanding that such information will only be used for that particular purpose.

Acquiring patient information is an integral part of the healthcare business, for both billing purposes and service delivery. Obtaining this information is not necessarily illegal, provided it meets the narrow requirements for maintaining patient confidentiality and the protection of patient information. However, should any personal information be accessed and/or published from a personal electronic device (e.g. a smartphone, iPad or personal computer), digital storage devices (iCloud, Dropbox, external hard drives)

or other data-capturing aids (notebooks or files), it can result in personal harm or defamation. In such an event, the initial information-acquiring person (the healthcare professional or staff member), also known as the responsible party, is directly to blame whether they are primarily responsible for publishing the information or not.[1] Therefore not only is the divulging of information (intentionally or unintentionally) illegal, but this also puts the onus on the responsible party to ensure that such information is protected.

According to the Health Professions Council of South Africa (HPCSA) guidelines on the protection of personal information,[6] a significant number of improper disclosures of patient information happen unintentionally. It is therefore important to understand the legal freedom and boundaries of the doctor-patient relationship. Healthcare professionals must be educated regarding the lawful processing of personal information, the rights of our data subjects (patients) and the consequences of careless handling of data. These are set out in the POPI Act.

What does POPI say?

Sections of the POPI act of note to the healthcare professional are included in this review. This summary cannot be regarded as a legal document, but merely as a guideline for healthcare professionals. It focuses on five areas from the act:

- lawful information processing
- the rights of the data subject
- what is considered personal information
- what recording of that information entails
- who can be seen as the responsible party.

Lawful information processing

Table 1 gives examples of illegal information processing. Lawful information processing[7] by the responsible party must include the following characteristics:

Table 1. Examples of illegal information processing

- Taking a photograph with your mobile device of a patient's wound (or any body part, for that matter) without his/her explicit consent
- Taking a photograph of the patient's hospital label and storing it on a mobile device, without formally safeguarding access to this information
- Storing patient information on any data-storage device/cloud/data bank, without restricted access
- Accessing patient information (e.g. blood results, radiography or medical notes) on a public computer and leaving it open
- Storing (on paper or in electronic files) patient information without any anticipated legal, research, or administrative value, for longer than 5 years

(*i*) Minimality: Information should only be processed to an extent that is adequate for the relevant purpose, for example, photographing only the section of the body that is being treated, not the whole body, or having a clerk acquire only information necessary to assist with billing and not intricate medical detail.

(*ii*) Informed consent from the data subject: This includes the principles of competence (mental and legal capacity), voluntariness (which includes autonomy, non-coercion and the right of objection) and disclosure of pertinent information (alternatives and risks). This can be in written or verbal form, but verbal consent must always be noted in the clinical notes. If data are intended for publication, written consent is compulsory.

(*iii*) Collection from the data subjects themselves: The data subject provides the information (and not a third party) to assure its accuracy.

(*iv*) Collection of data must be related to a specific function or requirement: For example, one might collect geometric data in order to plan pharmacological treatment, collect personal information for billing purposes or photograph a wound for treatment follow-up.

(*v*) Retention and restriction of records: The minimum duration for medical-information retention by law is 5 years. This may be extended for historical, statistical or research purposes. Personal records must be destroyed/deleted/de-identified as soon as reasonably possible. If someone were to gain access to records that have surpassed the retention period (older than 5 years), and information processing of those records was no longer a necessity for the primary purpose they were acquired for, the breach would be indefensible.

(*vi*) Reasonable security regarding the safeguarding, integrity and confidentiality of personal information: The processing of and access to personal information of data subjects must be restricted, and data subjects must be notified in the event of a security compromise. Reasonable security measures for an individual professional may not require the same level of sophistication as those for a large group practice.

The rights of the data subject

The rights of the data subject[8] include:

(*i*) Notification that personal information about him/her is being collected. This is an important principle of informed consent and can be done verbally or in writing. A patient has the right to know that information of any nature is being collected from him/her.

(*ii*) Notification if his/her information is accessed by an unauthorised person (anyone other than the responsible party), i.e. if a breach in security has occurred. This is compulsory in terms of section 22 of POPI, and there are very specific reporting steps that need to be taken. This can present an ethical dilemma, should a breach occur that no-one would know about unless you reported it yourself.

(*iii*) A request to correct, destroy or delete their personal information. This links to the principle of voluntariness during informed consent.

(*iv*) A reasonable objection to processing of their information.

(*v*) The submission of an inquiry or complaint to the Information Regulator if he/she suspects interference with the protection of personal information of any data subject.

Personal information

Personal information[9] is regarded as personal property, and includes:

(*i*) information regarding race, gender, sex, pregnancy, marital status, ethnic origin, sexual orientation, age, physical or mental health, disability, religion, culture, language and birth (date, place, time, etc.);

(*ii*) information regarding education and employment;

(*iii*) any identifying number, symbol or address; and

(*iv*) biometric information.

The POPI act does not apply to the processing of personal information of a purely personal nature (household activity), data that have been properly de-identified (where re-identification is impossible), or information that involves public safety (such as terrorist activity).

The act makes an exception for medical professionals and healthcare institutions regarding the prohibition against obtaining information relating to a person's health or sex life, since these are generally a necessity for proper treatment and care. However, acquiring this information outside the healthcare setting is deemed to be illegal.

Recording of personal information

Personal information[9] can be recorded by any of the following means:

(*i*) writing on any material;

(*ii*) recording or storing information by means of any data-capturing device;

(*iii*) using maps, plans, graphs or drawings of a personal nature, or which identify the subject in any way; or

(*iv*) using photographs, film, negatives, tape or another device in which visual images are embodied.

Responsible party

Recorded material must be in the safe possession of a responsible party.[11 This refers to a public or private body or person who determines the purpose of and the means of processing of personal information obtained from the data subject. In the healthcare setting this could be an individual healthcare professional, or a healthcare institution.

What does the HPCSA say?

Booklet 10 of the HPCSA's practice guidelines[6] deals with patient confidentiality, and clearly supports the protection of patient information. It is recommended that if the disclosure of patient information is necessary patient consent be obtained, disclosure minimised as much as possible, and anonymity must always take preference. The HPCSA recognises that a significant number of improper disclosures happen unintentionally, and stresses that clerks and receptionists should be trained in patient confidentiality and retention of disclosure.

The HPCSA states: 'Healthcare professionals should not discuss information about patients where they can be overheard or leave patients' records where they are vulnerable to disclosure, either on paper or electronically, where they can be seen by other patients, unauthorised healthcare personnel or the public. Healthcare practitioners should endeavour to ensure that their consultations with patients are private.'[6]

The recommendations made by the HPCSA state that each healthcare provider is responsible for the safeguarding of their patients' information. Stringent precautions should thus be taken to assure the security of the data storage unit used to store patient information, and 'if necessary, healthcare practitioners should take appropriate authoritative professional advice on how to keep information secure before connecting to a network. They should record the fact that they have taken such advice.' The same security requirements apply to the receiving or sending of patient information via fax, mobile device or email, as 'the data cannot be intercepted or seen by anyone other than the intended recipient.'[4] Healthcare practitioners should be aware of the fact that information sent by email may be intercepted.[6]

When can a healthcare professional be held liable?

The responsible party is guilty of an offence if:

(*i*) information was obtained without consent;

(*ii*) information was published or accessed by an unauthorised party;

(*iii*) reasonable harm or distress was caused to the subject;

(*iv*) the responsible party failed to take reasonable steps to prevent access to the information; or

(*v*) the responsible party failed to report a breach to the subject or the Information Regulator.

The penalty for a breach of privacy is related to the severity of the harm or distress caused. This can include termination of employment, sanctions by the HPCSA (including being struck off the roll of practitioners), a damages award of monetary compensation to the affected data subject (up to ZAR10 million) and imprisonment for a maximum of 10 years.[10]

Recommendations

Given the intended legislation, it is recommended that the following are considered:

(*i*) Always inform the patient if acquiring their personal information, notarising the consent if it was a verbal agreement. Written consent is necessary when information is disclosed or published. A reasonable suggestion is to have a discussion of these issues on the first consultation with a patient, and to notarise this discussion. This will not only properly inform the patient, but also safeguard the professional.

(*ii*) The recording of personal information should always be done accurately, preferably using information primarily from the data subjects themselves, and involve only the essential information as required for the specific purpose for which it is being collected.

(*iii*) When publishing patient information, always assure full de-identification. Written consent is still a requirement.

(*iv*) The retention of records and handling of patient information should be done securely, as recommended by the HPCSA guidelines.

(*v*) The deletion of the records after 5 years' retention is necessary, with the exception of records with historic or academic value, or those involving anticipated legislation.

(*vi*) The above steps should be executed in terms of a written POPI policy in the practice. The policy must be communicated to everyone who may have access to patients' private information in the workplace. This is one of the minimum reasonable measures expected by the Information Regulator.

Conclusion

The nature of the healthcare 'business' is personal and interesting. It is a normal human reaction for healthcare professionals to want to share their interesting cases and experiences with colleagues, and even friends and family. However, we are now forbidden by law to do so in any format, including on social media platforms. This requirement probably necessitates a significant change in the mindset of the medical fraternity, as the time-honoured sharing of information between colleagues cannot continue given the new legislation. Should personal patient information be leaked or published from a personal data-storage device, the responsible party or physician who acquired that information can be held liable for damages incurred. However, the threat of legal action should not drive the medical profession's attitude. We should support the legislation because it sets out in legal terms what we should already know is the right thing to do.

Acknowledgements. *The author wishes to acknowledge Prof. André Coetzee and Mr Gerhardt van der Merwe (Medical Protection Society), whose professional advice played a major role in the preparation of this document. She also wishes to extend her gratitude to Dr Pamela Scheepers for her help in grammatical correction, and Dr Willem Buys for his support.*

References

1. South Africa. Protection of Personal Information Act No. 4 of 2013. [Links]

2. Information Regulator (South Africa). http://www.justice.gov.za/inforeg/ (accessed 16 June 2017). [Links]

3. South Africa. National Health Act No. 61 of 2003.

4. Malefane M. Nurse fired over Zuma and wife Facebook rant. Sowetan Live, 3 July 2017. http://www.sowetanlive.co.za/news/2017/03/07/nurse-fired-over-zuma-and-wife-facebook-rant (accessed 7 March 2017). [Links]

5. Grobler C, Dhai A. Social media in the healthcare context: Ethical challenges and recommendations. S Afr J Bioethics Law 2016;9(1):22-25. https://doi.org/10.7196/SAJBL.464 [Links]

6. Health Professions Council of South Africa. HPCSA Guidelines for Good Practice in the Healthcare Professions. Confidentiality: Protecting and providing information. Booklet 10. Pretoria: HPCSA, May 2008. [Links]

7. South Africa. Protection of Personal Information Act No. 4 of 2013. Chapter 3: Conditions for lawful processing of personal information. [Links]

8. South Africa. Protection of Personal Information Act No. 4 of 2013. Chapter 2: Application provisions. [Links]

9. South Africa. Protection of Personal Information Act No. 4 of 2013. Chapter 1: Definitions and purpose. [Links]

10. South Africa. Protection of Personal Information Act No. 4 of 2013. Chapter 11: Offences, penalties and administrative fines. [Links]