Southern African Journal of Anaesthesia and Analgesia. 2021;27(6 Suppl 1):S69-72
https://doi.org/10.36303/SAJAA.2021.27.6.S1.2702

South Afr J Anaesth Analg
ISSN 2220-1181 EISSN 2220-1173

FCA REFRESHER COURSE

Social media and the Protection of Personal Information Act

R Lockhat

Private practice, South Africa
Corresponding author, email: *dr.rlockhat@outlook.com*

Keywords: social media, Protection of Personal Information Act, POPI Act

Although formulated in November 2013, the Protection of Personal Information (POPI) Act (No. 4 of 2013) came into effect in South Africa from 1 July 2021.[1] However, from as early as 2016–2017, the POPI Act was already active, mainly dealing with the appointment of the Information Regulator.[1] Following the proclamation of enactment of the POPI Act by President Cyril Ramaphosa from 1 July 2021, individuals and organisations have a year grace period within which to implement the necessary safeguarding measures before the enforcement of fines and prosecutions.[1,2]

The main purpose of the POPI Act is to **protect the processing of personal information by public and private bodies**.[3] Balancing the right to privacy against the reasonable right to access of information is vital in an era that supports both free access to information and personal exposure on social media and digital platforms. The Act bears importance for all South Africans, as it protects the distribution and prevents the abuse of personal information by individuals and organisations, domestically as well as internationally.[1]

Under the POPI Act, organisations are responsible for processing information in accordance with the conditions described under chapter 3 of the Act.[4] These principles contained in the POPI Act are similar to the data protection principles found under the European Union's General Data Protection Regulation[1,4] and are the following:

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

Sections of the POPI Act especially relevant to the healthcare professional are:[1,4]

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

Lawful information processing[1,4]

Lawful information processing consists of the following:

1. **Minimalism:** Information should only be processed to the extent that is sufficient for the relevant purpose. Examples of this include photographing only the section of the body that is being treated instead of the entire body, or having a clerk acquire only information necessary to assist with billing and not intricate medical detail.
2. **Informed consent from the data subject:** This includes several principles such as 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 information can be either in written or verbal form. However, verbal consent must always be noted in the clinical notes, and ideally, a witness should co-sign. If data are intended for publication, written consent is mandatory.
3. **Collection from the data subjects themselves:** The data subject (patient), and not a third party, provides the information. This ensures the accuracy of the information.
4. **Collection of data must be related to a specific function or requirement:** Data should be collected for a specific purpose. Examples include the collection of data in order to plan pharmacological treatment; the collection of personal information for billing purposes or a photograph of a wound for treatment follow-up.
5. **Retention and restriction of records:** The minimum duration for medical information retention by law is five years. This may be extended for historical, statistical or research purposes with permission from the data subjects or patients.[1] It is mandatory that personal records must be destroyed or deleted as soon as reasonably possible. If someone were to gain access to records that have passed the retention period (older than five 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.[1]
6. **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 breach. Reasonable security measures for an individual professional may not require the same level as those for a large group practice. However, necessary measures must be taken by the healthcare professionals and associated parties, such as billing companies, to ensure security of records.

Table I: Examples of illegal information processing[1]

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/databank, 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 five years.

Rights of the data subject

Based on the POPI Act,[4] the rights of the data subjects (or patients) are enforced through the following methods:

1. **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 about him/her. It is strongly recommended that written consent should be sought from a patient.
2. **Notification of the patient if his/her information is accessed by an unauthorised person.** This includes anyone other than the responsible party (the healthcare professional concerned), that is, if a breach in security has occurred. This is compulsory in terms of section 22 of the POPI Act, and there are very specific reporting steps that need to be taken. This can present an ethical dilemma when a breach occurs that no-one would know about unless you reported it. Any breach must be reported, as the implications of not reporting it are severe.
3. **A request to correct, destroy or delete their personal information.** This links to the principle of voluntariness during informed consent.
4. **A reasonable objection to the processing of their information.** Patients are well within their rights to object to the processing of their information provided it is a reasonable request.
5. **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[1,4]

Personal information is regarded as personal property and includes the following:

1. 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.)
2. Information regarding education and employment
3. Any identifying number, symbol or address
4. Biometric information

Exceptions are made with regards to the use of personal information **by the data subject for their own personal use**, information that is de-identified where re-identification is impossible or information that involves the safety of the general public (criminals, terrorists, etc.).

With regard to the medical and healthcare fraternity, only information that is pertinent to the treatment of the data subject or patient is allowed to be made available to the stipulated parties. This includes health information or sexual activity, if it will impact directly on patient treatment and care. In all other instances, using this information is illegal.

Recording of personal information

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

1. writing on any material
2. recording or storing information by means of any data-capturing device
3. using maps, plans, graphs or drawings of a personal nature, or which identify the subject in any way
4. using photographs, film, negatives, tape or another device in which visual images are embodied

Responsible party[1,4]

Recorded material must be in the safe possession of a responsible party, namely the public or private body or individual who determines the purpose 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.[1]

Regulations from the Health Practitioners Council of South Africa

There are a few similarities between the new POPI Act and current Health Practitioners Council of South Africa (HPCSA) practice guidelines regarding protection of patient information. Both emphasise the importance of patient confidentiality and support the protection of patient information.[3,4] The HPCSA booklet 10 strongly recommends that if the disclosure of patient information is necessary, patient consent must be obtained, disclosure minimised as much as possible, and anonymity must always take preference. The HPCSA further stresses that clerks and receptionists should be trained in patient confidentiality and retention of disclosure.[1,3,4]

The HPCSA is also similar to the POPI Act regarding the disclosure of patient information, both verbally and written to others who are not involved in the management of patients as well as electronic and paper records being readily available for others.[1,3,4]

The penalty for a breach of privacy is related to the severity of the harm or distress caused. This can include, but is not limited to, termination of employment, sanctions by the HPCSA (including being struck off the roll of practitioners), damages in monetary compensation awarded to the affected data subject or patient (up to ZAR 10 million) and imprisonment up to a maximum of 10 years.[1,3,4]

Intentional and unintentional exploitation of information

Personal information can be exploited either intentionally or unintentionally. Intentional publication of personal information in the healthcare setting is both unethical and illegal as it directly contravenes patient confidentiality.[1,4] A clinical example would be mentioning a patient or showing a photograph of a patient on social media or other public communication platforms. The roles and implications of social media in the healthcare profession are unfortunately still unacknowledged.[1]

All healthcare professionals and administrative staff acquire personal information on a daily basis. When a patient gives a medical history, they provide healthcare professionals with confidential personal information.[1] Legally, this information is regarded as a patient's personal property, which is divulged for a specific purpose, with the understanding that such information will only be used for medical treatment purposes.[1,4]

Social media, the POPI Act and implications in the medical world

With the establishment of the POPI Act and the COVID-19 pandemic, the escalation of telemedicine and e-HEALTH platforms has been insurmountable. Ward rounds, as well as medical meetings and patient-doctor consultations, have become virtual. This has improved accessibility, attendance and access that have not been possible before. However, with the increase of accessibility on virtual platforms comes the risk of security breaches. Attendees are able to take screenshots and pictures, and even record meetings, which can have significant security concerns if the essential security precautions are not taken.

The sharing of a variety of posts for businesses and practices has become increasingly popular on social media platforms. Social media has become the mainstay for advertising, marketing and education, ultimately boosting popularity and accessibility of information for both practitioners and patients alike. Specifically, with regard to medical practices, pictures may be used to demonstrate surgical skills and techniques, or may be used for interesting educational points for discussion on a worldwide platform, which may include some information of data subjects/patients. Frequently, these data subjects are unaware of the media and information that are taken and shared on the social media platform. According to both the POPI Act and HPCSA guidelines, it is mandatory for data subjects to give written consent to the responsible party before any data is published on social media, or distributed to others on email or messaging platforms.[3,4] At any point in time, the consent can be withdrawn by the data subject and the information provided can be withdrawn.

Furthermore, the responsible party is also required to appoint an information officer who will publish and ensure compliance with a POPI Act manual as read with section 51 of the POPI Act.[1,2,4] This would apply to all information used by organisations, private practices or individuals where information of the data subjects are used on social media platforms.

It is also important to emphasise the importance of the POPI Act and media messaging platforms. Care should be taken to ensure encryption codes and maximum security before any medical or patient information is shared. Security policies of messaging platforms should be assessed before these are used, particularly in sharing patient information and pictures. This also applies to social media security. Many social media users, whether on a personal or professional scale, do not read the terms and conditions associated with various platforms. As a result, they are subject to third party access to a host of information posted. This pertains to personal contact and location details, as well as payment details, which can be shared by third parties for advertising purposes.

Most social media platforms allow for the distribution of personal information to third parties without consent, resulting in both the person and the information shared through the platform being exposed. This includes information and pictures being open to be shared by third parties to others without consent from both the data subjects as well as the responsible party. In the event that information about a data subject is identified and they find out about the breach of the POPI Act, the responsible party (the party that originally posted the picture/information) will be found in contravention to the POPI Act and will be held liable. It is therefore imperative to ensure that privacy measures are implemented when signing in to social media platforms and that what is being shared is discreet, respecting integrity and anonymity of the data subject at all times.

There has been much confusion with regard to the sharing of personal pictures or social media posts. Section 6(1)(a) of the POPI Act states that the it does not apply to the **processing** of personal information in the option of a purely personal or household activity.[1,4] Therefore, personal posts of friends, colleagues and family are considered safe without POPI Act compliance.

The POPI Act does not define the terms 'personal activity' or 'household activity' – these will have to be interpreted on a case-by-case basis.[1,4] However, those who find their personal information posted on social media platforms without their consent are not without legal standing. Our common law, as codified in the Constitution, protects individuals' right to privacy on both a professional and a personal basis.[1,4]

Conflict of interest

The author declares no conflict of interest.

ORCID

R Lockhat https://orcid.org/0000-0002-2252-3203

References

1. Buys M. Protecting personal information: implications of the Protection of Personal Information (POPI) Act for healthcare professionals. SAMJ. 2017;107(11):954-6. https://doi.org/10.7196/SAMJ.2017.v107i11.12542.
2. Information Regulator (South Africa) [Internet]. Available from: http://www.justice.gov.za/inforeg/. Accessed 3 Aug 2021.
3. Health Professions Council of South Africa. HPCSA guidelines for good practice in the healthcare professions. Confidentiality: Protecting and providing information. Booklet 10. Pretoria: HPCSA; 2008.
4. South Africa. Protection of Personal Information Act No. 4 of 2013. Pretoria: LexisNexis; 2014.