deNovo Medica

Leader in digital CPD for Southern African healthcare professionals

Earn 3 free CEUs | Ethics

The POPI Act is here! What now?

A quick guide to POPIA-fying your practice

Presented by:

Elizabeth de Stadler
LLB LLM (Consumer Law)
Cape Town

Learning objectives

You will learn:

- The core concepts of the Protection of Personal Information Act (POPIA)
- The implications of the POPIA for health information
- How to identify the risks of POPIA non-compliance.

Introduction

Ten years of discussions about the Protection of Personal Information Act (POPIA) have left many healthcare practitioners weary of hearing or thinking about its implications. Ms de Stadler mischievously recommends that 'POPIA fatigue' be classified as a clinical term, as it makes one forget why this piece of legislation is so important, particularly in the context of healthcare. A more recent phenomenon, 'POPIA panic', is spreading rapidly as the cut-off date for compliance with the POPIA was 30 June 2021. Considering that healthcare practitioners are not privacy lawyers, Ms de Stadler considers the POPIA in the context of healthcare practice management and provides relevant, simplified and practical guidance to achieving compliance.

Click here to watch the full recording of the webinar

© shutterstock/439417594

Cipla

This report was made possible by an unrestricted educational grant from **Cipla**. The content of the report is independent of the sponsor.

What is POPIA about?

While privacy is a constitutional right and is protected by the POPIA, it is interesting that the POPIA often limits privacy as the right to privacy is not absolute

The POPIA is about balance. In terms of privacy, its preamble states: *'Protect the constitutional right to privacy including the unlawful collection, retention, dissemination and use of personal information;'* in terms of business, section 44(1)*(b)* states: '*But, the Regulator must take into account the interests of public and private bodies in achieving their objectives in an efficient way*.' While privacy is a constitutional right and is protected by the POPIA, it is interesting that the POPIA often limits privacy as the right to privacy is not absolute. There are many instances in which it is justifiable to infringe on a person's privacy; it is necessary for the Information Regulator to consider other interests of the public and private bodies in achieving their obligations or their objectives and to find the balance between necessity and proportionality. Is infringing on a person's privacy, e.g. by sharing their personal information with somebody else, necessary and is it being done in a proportional manner?

Privacy, information security and records management are the three foundations of the POPIA to which its principles are applied. Privacy concerns relate to what can be done with the personal information that has been collected, information security is about protecting the confidentiality and security of information from being compromised, and records management is concerned with what information may be kept as a record of activities. Core concepts of the POPIA are depicted in Figure 1.

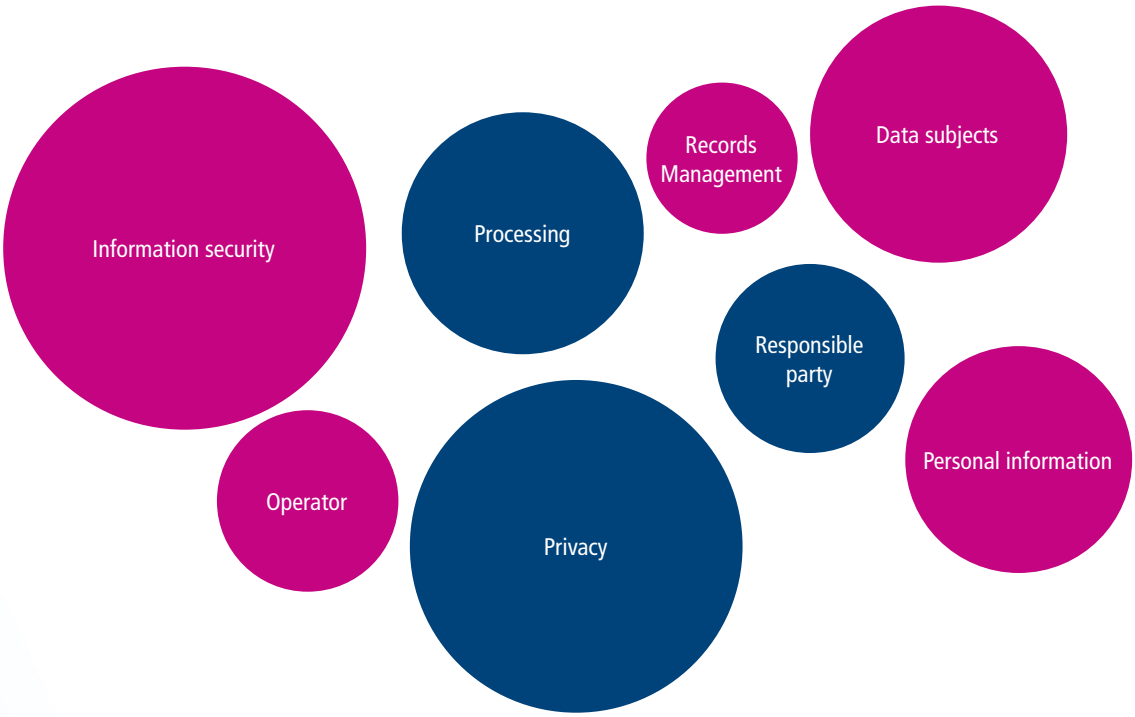

Figure 1. Core concepts of the POPIA

What is personal information?

Personal information is very broadly defined in the POPIA, and includes any information that can be traced back to an identifiable living natural person or an existing organisation

Personal information is very broadly defined in the POPIA, and includes any information that can be traced back to an identifiable living natural person or an existing organisation, although there is no finite list.

Personal information includes:

- Identifiers, e.g. identity number, medical scheme number
- Demographic information, e.g. gender, race, language
- Contact details, e.g. telephone numbers, email addresses, social media handles
- Financial information, e.g. bank account details, bank statements, salary
- Background or historical information, e.g. such as would be found in a *curriculum vitae*
- Usernames and passwords

- Biometric information – anything that is based on physical, physiological or behavioural characterisation
- Health information
- Preferences and opinions
- Behavioural information
- Correspondence.

Meet your data subjects

Many different types of data subject are encountered in the practice of healthcare. Patients and their families, employees and their families, employment candidates and partners in the practice are all considered data subjects, as are other doctors and affiliated organisations such as service providers, suppliers, independent contractors and any organisation practitioners work with such as hospitals, research institutions and biobanks. Research participants are also data subjects, and the Academy of Science of South Africa is currently spearheading the development of a code of conduct specifically with regard to the protection of personal information of research participants and how to find the balance between public interest in research and the privacy of the participant.

What is processing?

Many different types of data subject are encountered in the practice of healthcare

Processing activities lie at the heart of the POPIA. A processing activity is a collection of interrelated work tasks that achieve a specific result during which personal information is created, collected, used, shared, transformed, stored or destroyed; examples of different processes include creating a profile on the system when onboarding a new patient or submitting samples for testing.

The POPIA requires the security of personal information to be protected throughout its life cycle and therefore prescribes rules for each part of each process based on the three components of confidentiality, integrity and availability (Figure 2). Confidentiality is about ensuring that only people who need to can access that information. Integrity is about ensuring that the information is accurate, particularly in the healthcare context where inaccurate information can literally mean the difference between life and death, and that it has not been altered, tampered with or become corrupted. Availability is not only about ensuring that the personal information cannot be hacked, but also about ensuring that the information is properly backed up so that it will not be lost.

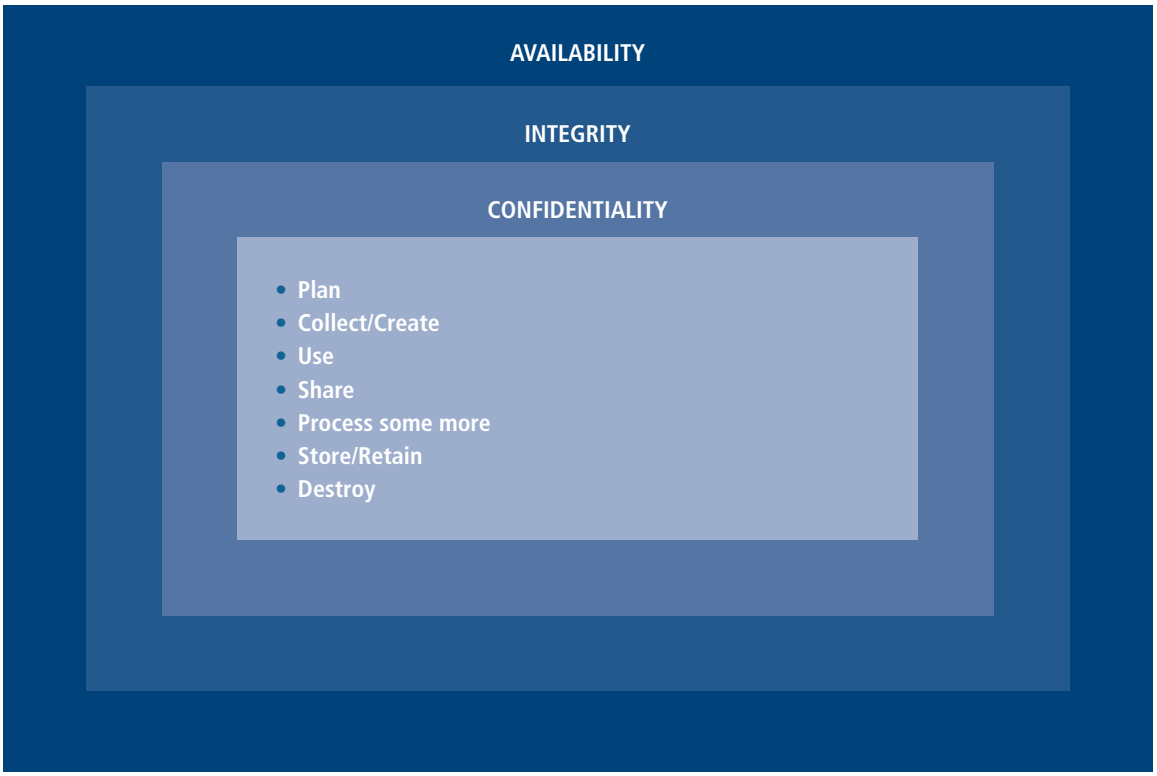

Figure 2. Processing activities lie at the heart of the POPIA

Who is the 'responsible party' and who is the 'operator'?

Different organisations and different individuals process personal information together. For example, a hospital as the 'responsible party' will have certain rules regarding POPIA compliance that a doctor who has rooms in that hospital must align with; in this case, the doctor is the 'operator'. In essence, an operator is someone who processes personal information on behalf of the responsible party.

In light of the stringent regulations that healthcare professionals have always had to adhere to, the requirements of the POPIA are perhaps less alarming than for those who are in unregulated industries

Health information in the POPIA – crib notes

Section 32 of the POPIA deals specifically with health information and allows for the sharing and use of personal information in an emergency. Currently, the POPIA has broad exemptions for health research, as long as it is performed in an ethical and responsible manner, and has even catered for the COVID-19 pandemic whereby the government has six weeks to anonymise the 'track-and-trace' database once the state of disaster has been lifted. In light of the stringent regulations that healthcare professionals have always had to adhere to, the requirements of the POPIA are perhaps less alarming than for those who are in unregulated industries.

Perform a POPIA risk identification

Table 1 summarises the principles of the POPIA that are important for the healthcare professional. It outlines their responsibilities and how to document their compliance.

Table 1. Risks for POPIA non-compliance

The question	Signs of trouble YOU ARE NOT ON TOP OF THIS!
Know who is accountable Are you sure that you know who the responsible party is and who the operator is?	• There is sharing, but no contract • There is a contract, but it does not state who the responsible party is
Document compliance Is the processing activity written down?	• You cannot find out how it works • The process has not been documented; or • It has been documented, but not recently
Purpose specification and provide a legal basis? Is this legal? Has someone checked that you have a legal basis?	• Purposes have not been specified in writing • Legal basis has not been documented
Keep processing to a minimum 'Less is more' is a key principle of the POPIA. Are you over-collecting or over-processing?	• You have not done a form analysis • You did not ask 'What do we use this for?' for each field • You collect the same information over and over • You have not asked 'How we can do this more efficiently?'
Obtain information from legal sources Where did we get the personal information from? Is it legal?	• You do not know where the information comes from • You have not assessed whether the alternative source is legal

Transparency 'No surprises' is a key principle of the POPIA. Do data subjects know what you are doing with their information?	• No privacy notice, no processing! • You have not checked that there is a privacy notice and that it covers the process in question • There is a privacy notice, but data subjects do not know about it
Ensure information quality Ask 'How do we make sure that information is (and stays!) complete, accurate, up to date and not misleading?'	• You collect information over and over again • Your systems do not speak to each other • You do not practise master data management (or know what it means) • You do not assess the quality of the information
Limit sharing Name the 'third parties' (people other than us or the data subject) with whom data is shared. Do you have contracts in place with these third parties?	• You do not know who data is shared with (there is no record) • You have not determined whether it is legal to share the information • You know there is sharing, but there is no record of a contract or you do not know whether there is a contract • There is a contract, but it does not say anything about how the personal information should be handled and what it can be used for
Keep the information secure Is the information protected against breaches of confidentiality, failures of integrity and interruptions of availability?	• You think that security is the responsibility of the IT department (so the process has not been assessed) • Information assets are not part of your business continuity plans • You do not have processes that control changes to personal information (anybody can update personal information)
Records management When does the relationship with the data subject end? For how long do you need to keep the information in use? Once it is not 'in use', what records do you need to keep?	• You keep everything forever • You can never find anything • When you find it, you do not know which version it is • Your records retention schedule is a list of legislation with retention periods
Data subject participation Can you process the following requests accurately and quickly? • What information do you have about me and who has access to it? • Delete my information! • Please correct my information • I want to object to how you are processing my information • I want to withdraw the consent I gave • I want to make representations about an automated decision	• You do not know what information you keep where, what you use it for and who you shared it with • There is no process to update information in all of the places it is stored (master data management) • You do not have a process to handle data subject requests • Consents are not managed in a central place • You do not know when you are allowed to delete information

Protecting the security of personal data is the bigger challenge, as most healthcare professionals are already compliant with the other aspects of the POPIA anyway

Procrastination – where the risk usually lies!

Although procrastination is often perceived as being about laziness, it is usually more about fear of failure. People tend to procrastinate about things they know the least about and in terms of the POPIA, healthcare professionals tend to procrastinate about the technical elements. Ms de Stadler warns that it is very difficult to recover from an information security incident, whereas for breaches of most of the other aspects of the POPIA the Information Regulator will caution and advise. She feels that protecting the security of personal data is the bigger challenge, as most healthcare professionals are already compliant with the other aspects of the POPIA anyway.

Check your security – now!

The 2019 Verizon Data Breach Investigations Report records 43% of cyber-attack victims as being small businesses and that within the previous 12 months, 47% of small and medium businesses had suffered from a cyber-attack with an average cost of $200 000. A useful checklist for optimising cyber security can be sourced at The Ultimate Small Business Cyber Security Checklist | SugarShot.

Key learnings

- The POPIA is about finding the balance between proportionality and necessity when considering the use of personal information
- Privacy, information security and records managements are the three foundations of the POPIA
- Personal information is very broadly defined
- Many different types of data subject will be encountered in the practice of healthcare
- Security of personal information must be protected throughout its life cycle
- The principles to consider when performing a risk identification for POPIA non-compliance.

This summary report was compiled for *deNovo Medica* by Glenda Hardy, BSc (Hons) Medical Cell Biology, from the transcript based on the webinar presented by Elizabeth de Stadler

Published by
© 2021 deNovo Medica
Reg: 2012/216456/07
70 Arlington Street, Everglen, Cape Town, 7550
Tel: (021) 976 0485 | info@denovomedica.com