

**CONFIDENTIAL**

# POPI and your Practice: How the new privacy law affects you

---

SASLHA Webinar

Zoom

10 June 2021

Presented by

Esmé Prins-Van den Berg



**HEALTHCARE**  
NAVIGATOR

---

---

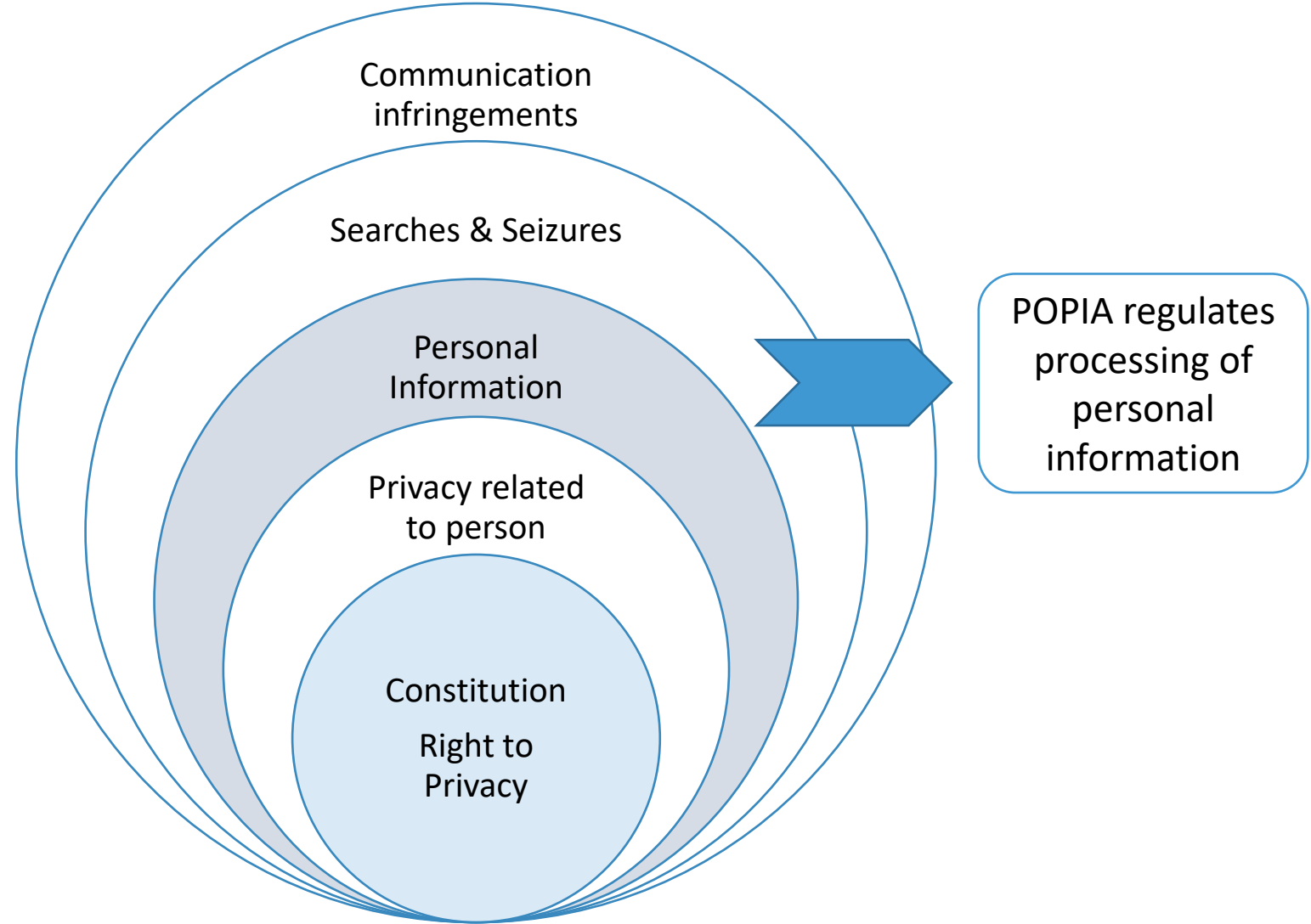
# Protection of Personal Information Act (POPIA) will become enforceable with effect from **1 July 2021**

Non-compliance could have significant  
consequences for practices

What is it all about?

# POPIA

---





## Processing

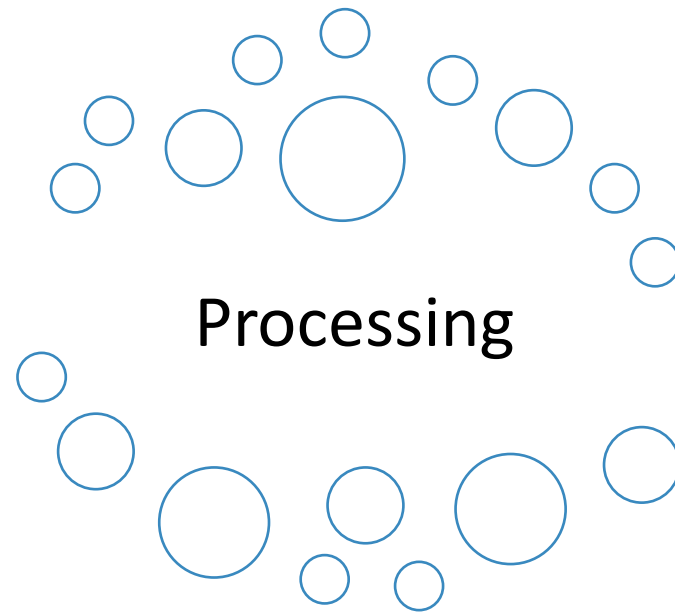
Includes collection, receipt,  
use, storage,  
dissemination, destruction  
of personal information

Disclosure - PAIA

## Personal Information

Includes age, gender, race,  
contact details, health  
information, employment  
history, opinion about  
person, preferences or  
opinions of person

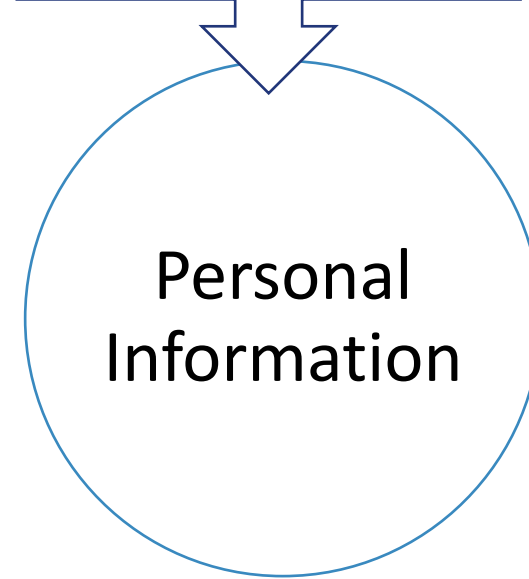
Names – not always



Includes collection, receipt,  
use, storage,  
dissemination, destruction  
of personal information

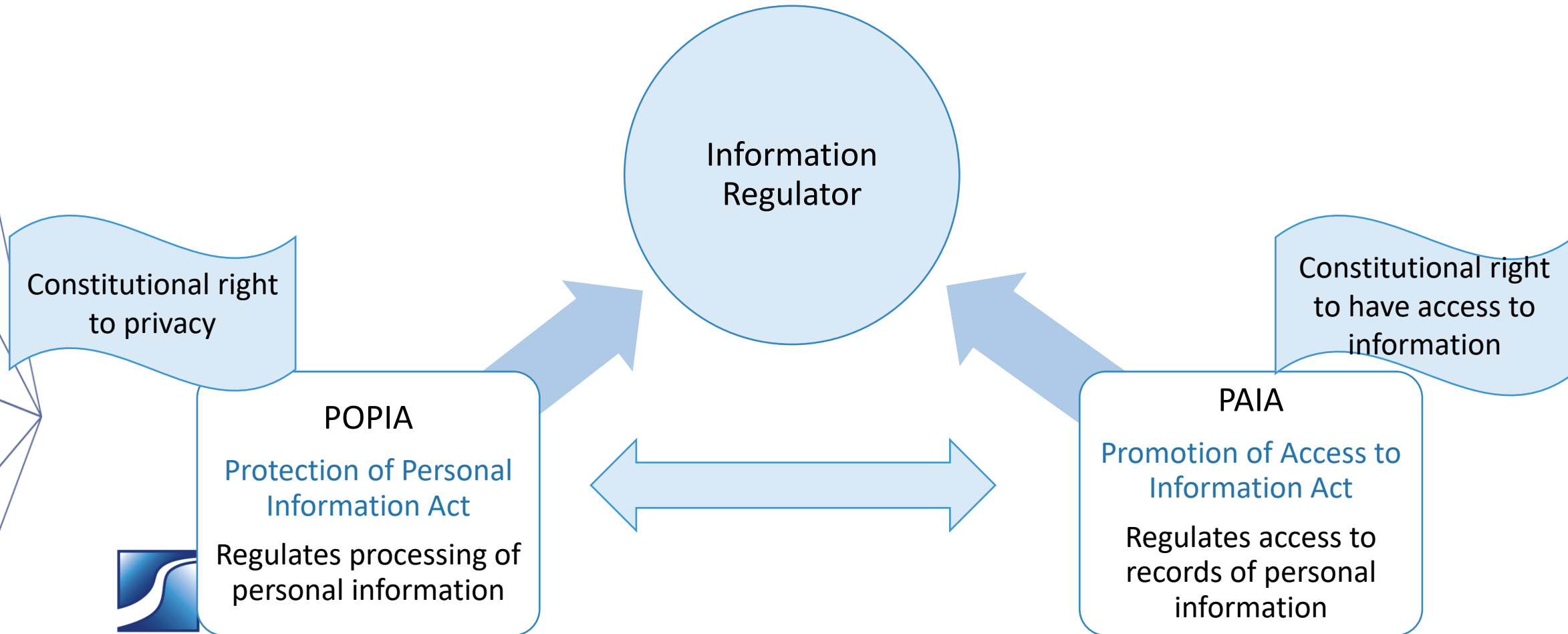


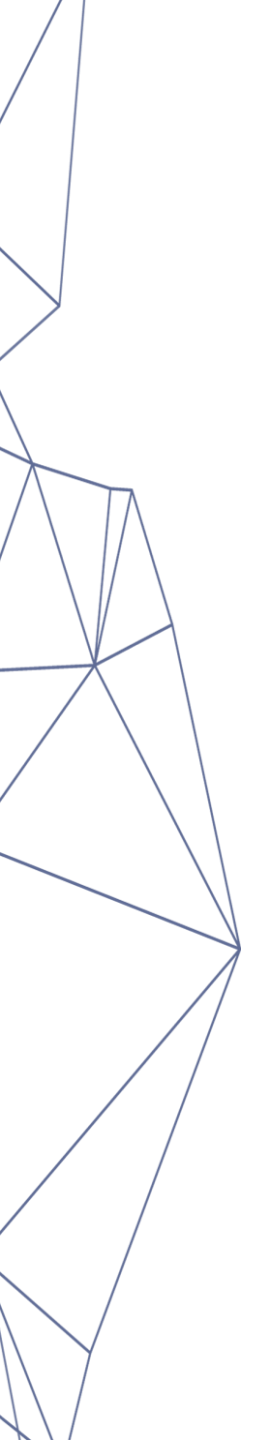
Data Subjects  
(living human beings  
and legal persons)



Includes age, gender, race,  
contact details, health  
information, employment  
history, opinion about  
person, preferences or  
opinions of person

# POPIA, PAIA and the Information Regulator



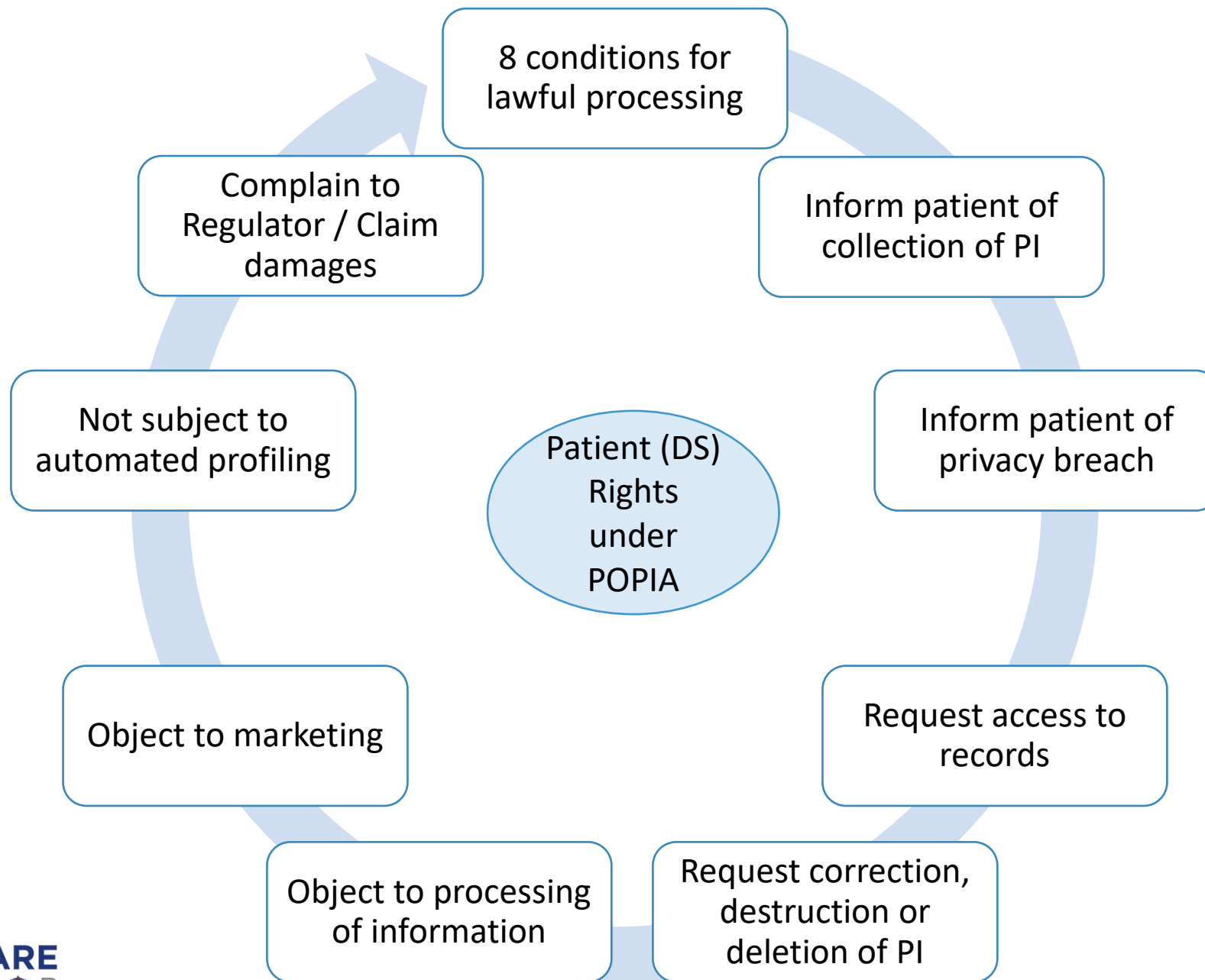


---

# Data Subjects' Rights

## (Patients' Rights)





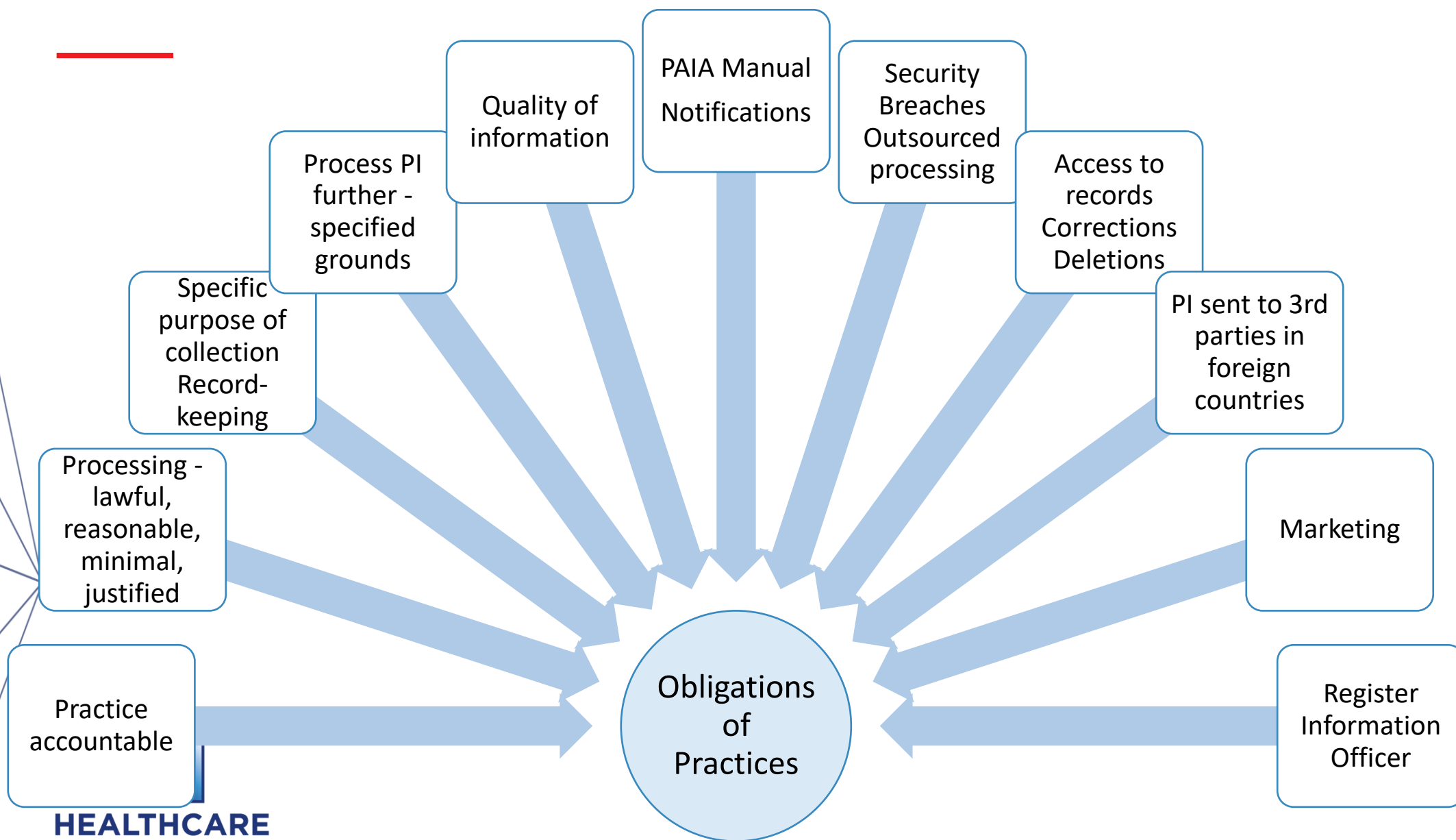


---

## Data Subjects' Rights



## Obligations of Responsible Parties



---

Every processing activity related to PI may *only* occur on a legal basis  
listed in POPIA

For example, authorised by legislation, with consent, etc.

Different options depend on type of PI

When do you need consent?

# Justification for Processing: Patients

---

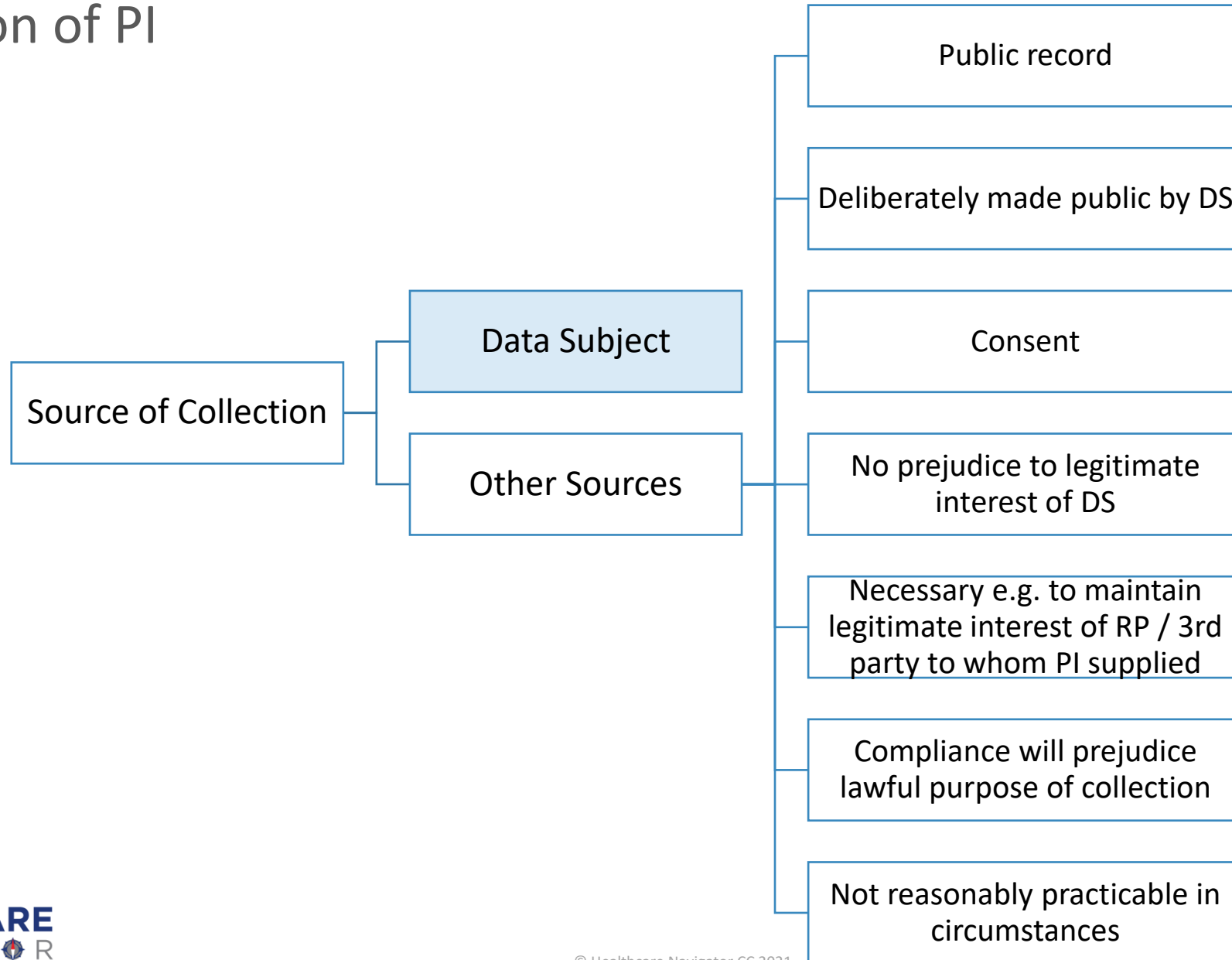
- Permissions to process information in legislation
  - Obligation to keep medical records (National Health Act)
  - Health and race-related information: May process for treatment and care of patients (POPIA)
  - Health information (ICD10 codes): May process for practice administration (POPIA)
  - Contact details, addresses and ID numbers of patients / authorised persons may be processed to accept patients (contract concluded) (POPIA)
- Legitimate interest of patient or practice in certain instances acceptable (not special or children's information) (POPIA)

# Justification for Processing: Patients

---

- What else do you do with personal information of patients? For example, disclosures
- If processing activity is *not* authorised by legislation, obtain consent
- Consent must be voluntary, specific and informed
- Children of consenting age: Independent consent, otherwise parental / authorised consent
- Consent can be withdrawn - manage
- If you rely on consent you have the burden of proof

# Collection of PI



# Record Retention

For as long as  
necessary to achieve  
purpose of collection  
& processing →  
destroy, delete, de-  
identify

unless

Law

Lawful purpose

Contract

Consent

Historical Statistical  
Research

Record used for  
decision about DS

Law / Code of Conduct

Allow DS reasonable  
opportunity to access

Consider  
HPCSA's  
guidance



# Data Subjects: Right to Know

Reasonableness  
Transparency

When?  
How?

Who?	<ul style="list-style-type: none"><li>• RP Details</li><li>• RP collects PI</li></ul>
What?	<ul style="list-style-type: none"><li>• Nature of PI</li><li>• Voluntary / Mandatory + consequences</li></ul>
From whom?	<ul style="list-style-type: none"><li>• Source of collection</li></ul>
Why?	<ul style="list-style-type: none"><li>• Purpose</li><li>• Law authorising</li></ul>
Whereto?	<ul style="list-style-type: none"><li>• Across RSA borders?</li><li>• Level of protection</li></ul>
To whom?	<ul style="list-style-type: none"><li>• Recipients</li></ul>
DS rights	<ul style="list-style-type: none"><li>• Access / Object (legitimate purpose) / Correct / Delete</li><li>• Complain at IR</li></ul>

What must be done?

# Compliance Framework

- ☐ Identification of lawful bases of
  - ☐ Processing and further processing - Know when you require consent
  - ☐ Collection from 3<sup>rd</sup> parties - Inform patients / other data subjects
  - ☐ When sending PI to 3<sup>rd</sup> parties in foreign countries - Notifications to Regulator, if required
- ☐ Disclosures of information must be authorised
- ☐ Manage consent
- ☐ Only collect information required for lawful purpose (review patient documentation)
- ☐ Notifications to patients and other data subjects (e.g. Privacy Policy)
- ☐ Only keep records for as long as lawful (Record-keeping Policy)
- ☐ PAIA Manual

## Compliance Framework

- ❑ Outsource agreements ('operators'): Implement written agreements containing prescribed clauses
- ❑ Impose confidentiality undertakings on employees and support persons with access to personal information
- ❑ Implement processes e.g. requests for access to records / deletions / corrections, investigation and reporting of privacy breaches
- ❑ Record access to information requests and recipients of personal information
- ❑ Secure record-storage (files and electronic records)

# Compliance Framework

---

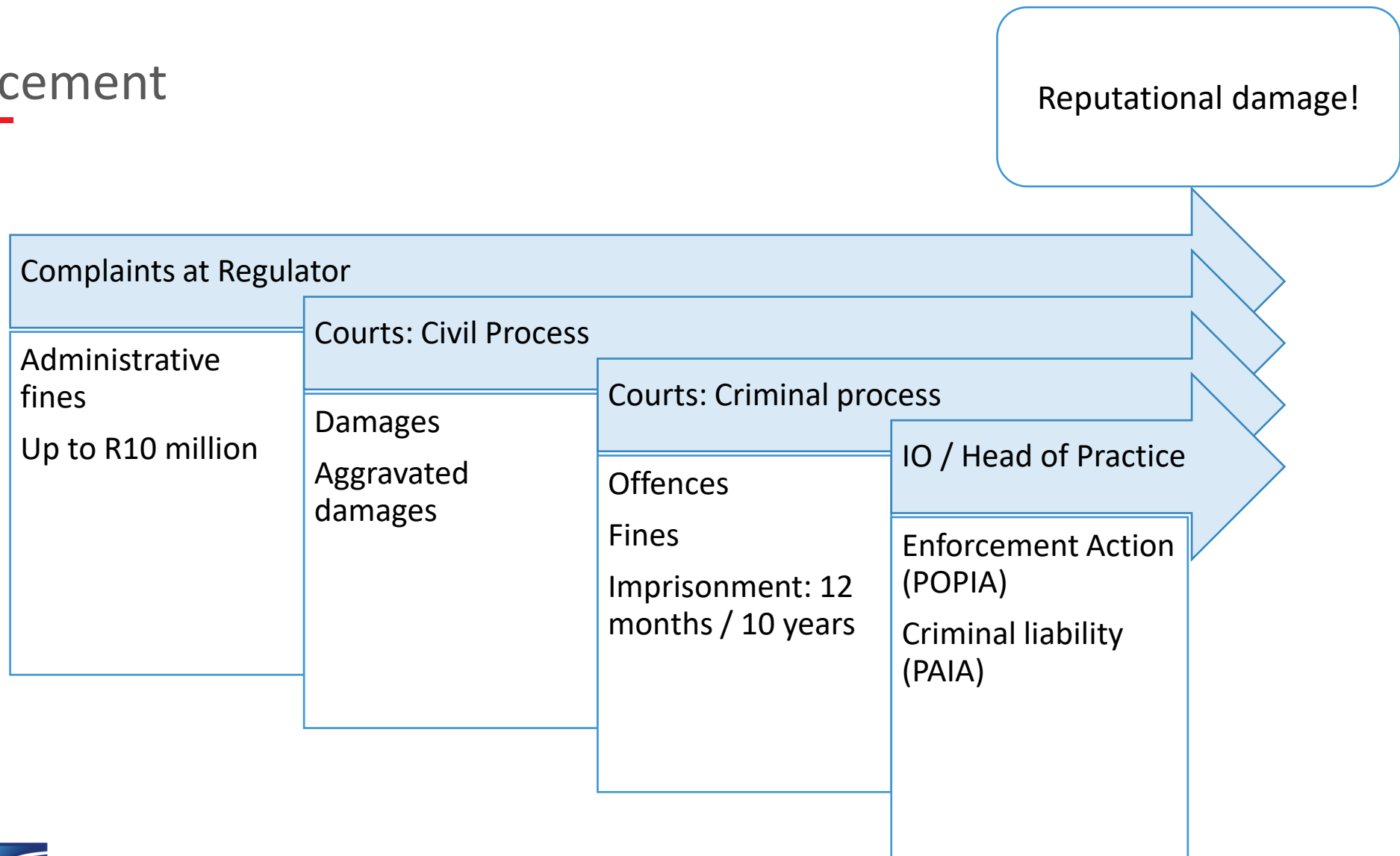
- ☐ Security of systems and processes [People, Processes, Systems]
  - ☐ Reception
  - ☐ Emails
  - ☐ What's App
  - ☐ System hacking (back-ups)
- ☐ Implement POPIA compliance framework
- ☐ Personal information impact assessment
- ☐ Training of and guidance to employees
- ☐ Register Information Officer at Information Regulator

# Be Practical

Social media, What's App	Permanent destruction – hard copy and electronic information (secure shredding)
Photos and videos	Old laptops – wipe hard drives
Mobile phone – lock	Discussions containing PI
Encryption of computers	Shared printers
Passwords on documents?	Change passwords regularly
USB Memory Sticks	Dropbox / Google Drive / We Transfer
COVID Registers	Content of records (Notes)

# What is the Down-Side of Non-Compliance?

# Enforcement





# Case Studies: Privacy Breaches

Access to records only if required for job / function

85 employees at hospital had access to patient file of celebrity -  
Insufficient security of medical records

## Record-Keeping Periods

1. Data retention periods not defined
2. Personal data not deleted when no longer required
3. Data not erased and corrected at request of data subject

## Access to Record Requests

1. Not giving access to personal data
2. Not providing easy means of accessing data
3. Placing unreasonable limits on number of requests per individual
4. Allowed customers to access their PI (hard copies) only once per year

## Security of Records

1. 500 000 patient records left in unsecured location (unlocked crates, disposal bags and cardboard box in rear courtyard of premises)
2. File with login credentials of 35 000 students and employees found in public storage area

Where to from here?

## Everything is not New

- Practitioners are used to confidentiality requirements: Ethical Rules, legislation
- Technology, inter-connectivity and abuse of information by persons and entities resulted in new data protection legislation being implemented globally

*‘When information is in motion, you loose control’*

- The bar has now been raised for the handling of personal information

**Online cybersecurity threats > 600 per minute!**  
**Health care industry: High risk**

**UK (July – Oct 2020):**  
**Most common cybersecurity incidents: Phishing**  
**Most common cause of data breaches: Misdirected emails**

# Legislation and Guidance Notes Published by Information Regulator

- POPI: Act and Regulations
- PAIA: Act
- Guidance Notes by Information Regulator
  - Prior Authorisation
  - Information Officers
- IO Registration <https://www.justice.gov.za/infoereg/portal.html>

<http://www.justice.gov.za/infoereg/>



# Conclusion

---

- Intention of POPIA not to prevent health professionals from conducting their practices
- Patients may use and abuse POPIA!
- Human behaviour: Try to minimise human errors
- Compliance with POPIA is not a 'document file'
- Compliance with POPIA must become integral to practice - culture
- Every person important to achieve compliance...weak links...risk

POPI Toolkit™ for healthcare  
practitioners available at  
[www.healthcarenavigator.co.za](http://www.healthcarenavigator.co.za)

# Questions / Discussion

# Thank you

---

Healthcare Navigator cc

[esme@healthcarenavigator.co.za](mailto:esme@healthcarenavigator.co.za)

+27 83 381 6428

[www.healthcarenavigator.co.za](http://www.healthcarenavigator.co.za)



**HEALTHCARE**  
NAVIGATOR

---