POPIA in the health context: the legal position

Prof M Labuschaigne
School of Law
University of South Africa
25 August 2022

36th South African NATIONAL BLOOD Transfusion Congress
22 – 25 August 2022 - Durban
SHAPING A SUSTAINABLE FUTURE

UNISA college of law

Overview

- Introduction
- Privacy breaches in health care
- Legal framework
- Privacy challenges arising from personal health information & sharing
- Unpacking POPIA
- Draft POPIA Code of Conduct for Research
- Data Access Committees and DTAs
- Conclusion

Privacy breaches in health care

UNISA college of law

Privacy breaches

2015 – 2019:

76.59% were in the healthcare sector; 3x more than breaches in education, finance, retail, and government sectors combined*

- **Healthcare data is more valuable on the black market than financial data:**
  - financial data is shut down quickly;
  - healthcare data can be used to commit identity theft for much longer;
  - Healthcare sector has larger databases –more attractive targets;
  - More intermediaries processing health data.

*https://www.hipaajournal.com/healthcare-data-breach-statistics/

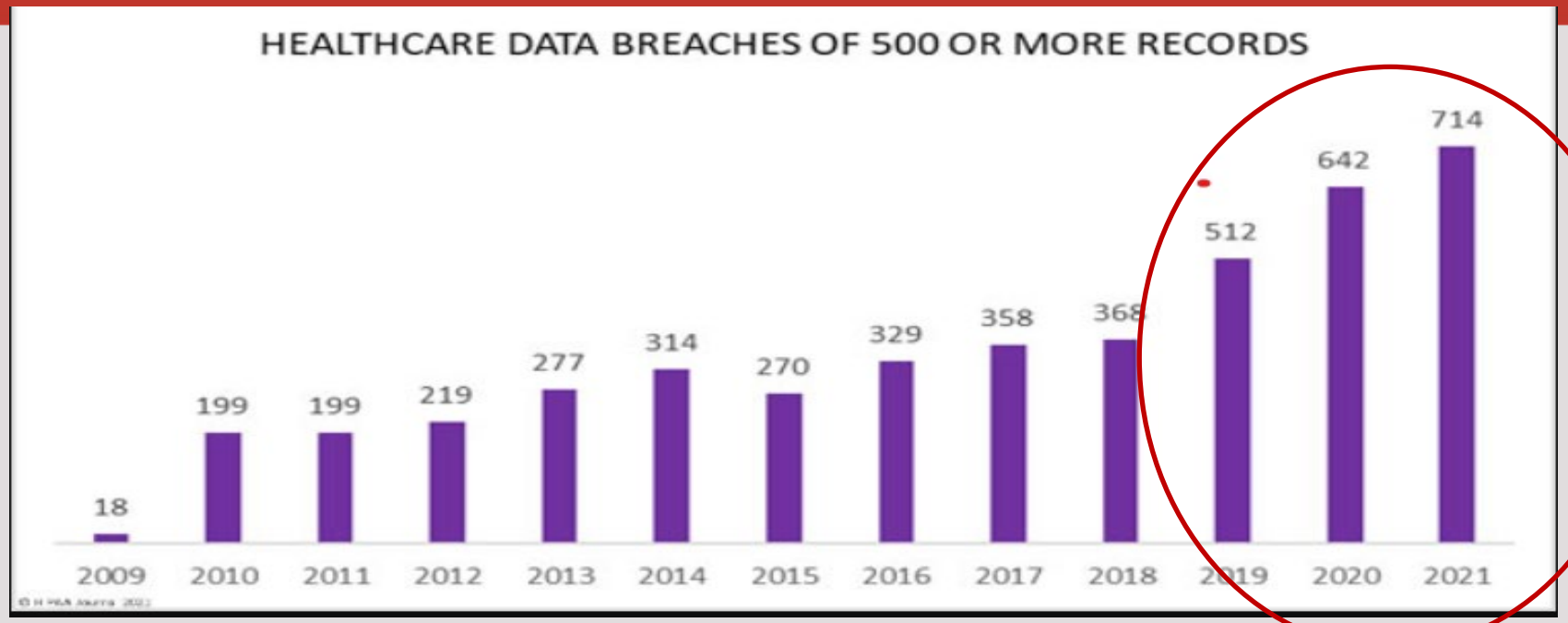
Australia's biggest health data breach

Australian Red Cross Blood Service's health data breach = Australia's biggest data breach ever:

- A file containing information (including at-risk sexual behaviour) relating to approximately 550,000 prospective blood donors was saved to a publicly accessible portion of a webserver managed by a third party provider
- This was an inadvertent error by an employee of the third party provider

UNISA college of law

Increase in health care data breaches



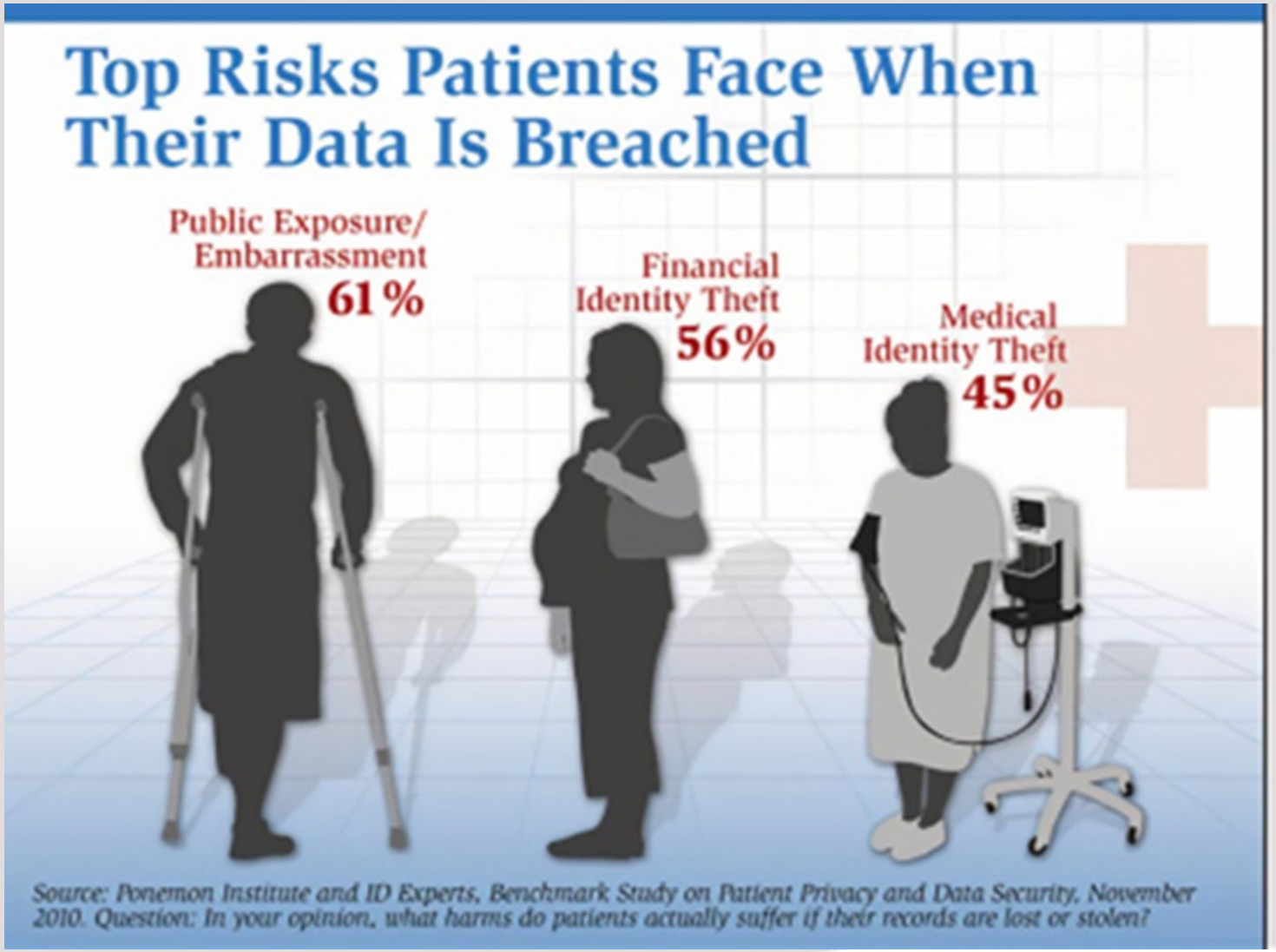
Between 2009 and 2021, 4,419 healthcare data breaches of 500 or more records were reported to the HHS' Office for Civil Rights, involving the loss, theft, exposure, or impermissible disclosure of 314,063,186 healthcare records.

This equates to more than 94.63% of the 2021 population of the United States.

https://www.hipaajournal.com/healthcare-data-breach-statistics/

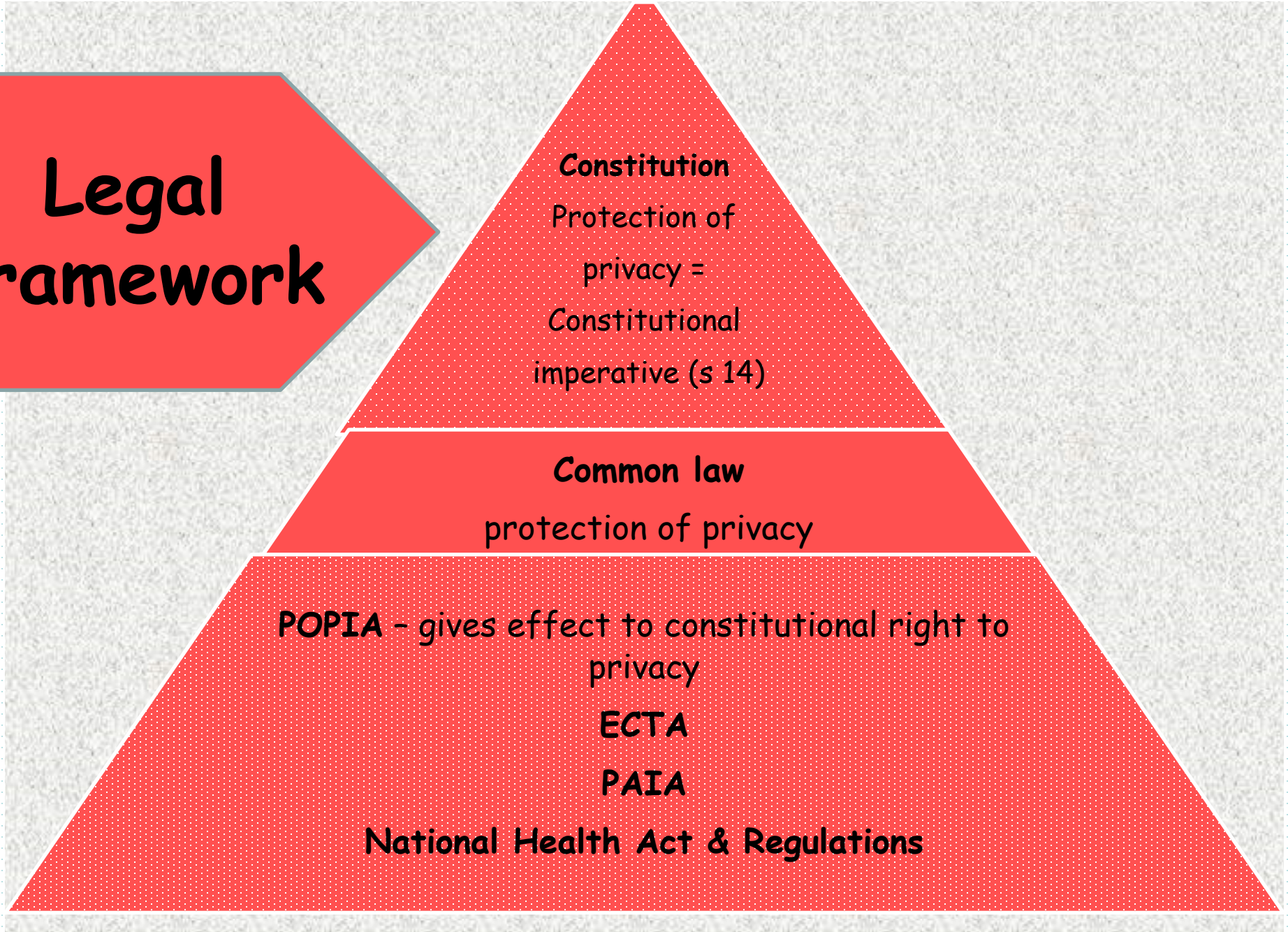
UNISA college of law

Multiple risks: Patient privacy and data security survey



UNISA college of law

Legal framework



Privacy challenges: consent

- Inadequate
- Difficult to predict **who will access data; for which purpose, and under what conditions** in the future
- **Not clear what data will reveal about research participants** (incidental findings)
- **Future use in research uncertain** at time of obtaining consent; re-consent required?
- ***Not possible; practical or feasible****; costly to obtain re-contact and re-consent*

Challenges (cont.)

- **"Open science"** & expediency arguments favour other types of consent (broad consent or tiered consent models) for donation of samples
- **NB: Consent for donation of samples not the same as consent for the processing of personal information**
- SA legal framework: **different consent requirements for research; clinical practice; protection of PI**:
  - the manner consent is obtained
  - recording of the consent
  - specifics that should be included/disclosed when obtaining IC (standard of disclosure)

Challenges (cont.)

Research

Written consent of person after he/she has been informed of the *objects of the research and of ANY possible positive or negative consequences to his/her health*

S 71 of NHA

"Health service"

Informed consent required (full knowledge)
Ss 6,7,8 of NHA

Common law standard of disclosure for IC: *Castell vs De Greef* case

Health service for research purposes
informed written consent & prior authorisation by doctor, REC and head of health establishment
S 11 of NHA

Challenges (cont.)

NHA:

Removal of tissue, blood, blood products or gametes from living persons –

Written consent

S 55

NHA:

Donation of human tissue & bodies from deceased persons

Consent in a Last Will; document; or proxy consent providers to consent in specific order – s 62

POPIA: Processing of PI, SPI

Specific, voluntary and informed consent; directly collected from consent giver; explicitly defined & lawful (Note: not required to be in writing)

S 13

UNISA college of law

Challenges (cont.)

- De-identification and re-identification of data
- **Can genetic data ever truly be de-identified, and if so, what are the conditions under which the de-identification will be** irreversible? Triangulation with other data sets & publicly available data?
- **Biobanks**:
  - eg funder requirements may require audited case report forms containing participant's PI, which may link a participant to specific genetic information;
  - or researchers may find that a participant's health is at risk and re-contact may be the ethical route

POPIA

- Omnibus & general legal framework regulating processing of personal information
- **Eight conditions must be met for the lawful processing of data**
- POPIA applies to all personal information of all **'identifiable, living, natural person'** (Section 1).
- **Not applicable to information that has been de-identified to the extent that it cannot be re-identified** again (section 6) = anonymised data

Balanced approach

- Purpose of POPIA (s 2): protection of PI is subject to **other important rights and interests**, one of which includes the 'free flow of information within the Republic and across national borders'
- **Balance be struck - between protection of PI and promotion of science and free flow of information** across borders (also constitutional right to scientific research)
- ***A purposive interpretation*** is followed when SA Acts of Parliament are interpreted, which supports the conclusion that other consent models are possible under POPIA, provided that proper research governance is in place (eg REC)

Data subject and responsible party

- '**Responsible party**' (RP) = public or private body or any person which alone or in conjunction with others, determines the purpose of and means the processing of personal information
- Must ensure that the research complies with POPIA and the Code of Conduct for Research (still draft)
- **Data subject** (DS) = the person to whom the personal information relates
- A research study may have multiple RPs and DSs

What is personal information?

- Very wide definition in POPIA
- Any **identified or identifiable information** relating to "an **identifiable, living, natural person**"
- **Irreversibly anonymised data – not PI**
- If de-identified or pseudonymised, but re-identifiable = still personal information under POPIA? POPIA not clear, but this should be PI
- Categorising information as personal or non-personal **depends on the context**: **the same data point can be personal or non-personal**, thus subject to the strict processing requirements of POPIA (or not)

UNISA college of law

What is personal information? (cont.)

- Forecasts: global data sphere will have grown from 33 zettabytes in 2018 to 175 zettabytes in 2025

  (1 zettabyte = 10^{21} bytes or a trillion gigabytes)
- Advances in data analysis techniques and accessibility to data - **no longer difficult to establish a connection to the person from whom the data originated**
- Thus, we could find ourselves in a situation (in the not too distant future) where **most types of data have the possibility of being personal information and therefore subject to privacy regulations**

Purpose of collection

- Specific purpose; is adequate, relevant and not excessive (s 10)
- **Collected directly** (s 12(1)) for a '**specific, explicitly defined and lawful purpose**' (s 13)
- **Exceptions to above:** consent to collection from another source or where compliance not reasonably possible (s 12(2))
- Further processing: **compatible with the purpose for which it was collected** (s 15(1)), e.g only be used for research for which it was obtained
- **Other purposes:** **used for research and the personal information will not be published in an identifiable form** (s 15(3)(d)(e))

UNISA college of law

Processing of special personal information

- **General prohibition on the processing of special personal information** that includes health and genetic data (s 26)
- **May be processed if the data subject:**
  - **consents** (s 27(1)(a)),
  - processing is for research that **is in the public interest** (s 27(1)(d)(i));
  - or the **processing is for research and it would 'be impossible or would involve a disproportionate effort to ask for consent'** (s 27(1)(d)(ii));
  - the data subject **has made the information public** (s 27(1)(e))

Processing of special personal information

- If processed under the public interest or for research: '**sufficient guarantees**' that the **processing does not adversely affect the privacy** of the data subject **to a disproportionate extent**
- Information Regulator **may authorise the processing of SPI upon application, provided that such use is in the public interest** and safeguards have been put in place by the responsible party (s 27(2)).
- How and by whom these 'safeguards and guarantees' are to be provided, still not clear (to be clarified by the draft **Code of Conduct)**

UNISA college of law

Processing limitation: SPI (cont.)

- Prohibition on processing of PI not applicable if processing done by (s 32):
  - medical professionals, healthcare institutions/facilities or social services **if necessary for the proper treatment and care of the data subject; or**
  - insurance companies, medical aid schemes, pension funds, employers etc, **if the processing is necessary for their lawful activities.**
- PI may only be processed **subject to an obligation of confidentiality by virtue of profession, legal obligation**, etc, or established by written agreement between the responsible party and the data subject

Processing limitation (cont.)

- PI concerning **inherited characteristics** may not be processed **unless** (s 32(5)):
  - a serious medical interest prevails; or
  - the **processing is necessary for historical, statistical or research activity**

  * Lack of clarity regarding IC: to be addressed by the ASSAf Code of Conduct from IR for processing of PI

Personal information impact assessment

- All research must go through a **Personal Information impact assessment ('Research PIIA')** to ensure responsible parties manage the risk to research participants appropriately by including appropriate safeguards in research protocols
- Research PIIAs are not performed per Research Institutions and Independent Researchers, but **performed per research activity**, eg project/study
- Research PIIA should follow the approach taken in the European Union, where only high-risk Research requires **a complete Gap Analysis**

Research PIIA (cont.)

- **Three-phase Research PIIA:**
  - Preliminary risk assessment (to determine high-risk research) – see 11 questions next
  - Gap analysis (is research protocol complying with POPIA?) – if high risk processing
  - Implementation and monitoring (to record safeguards and a monitoring plan in the research protocol); if high-risk, IO must approve research protocol & monitor compliance at least every 2nd year

How to determine high-risk activities

If there are more than six YES answers to the following eleven questions, the activities could be **considered high-risk. This scoring exercise = the minimum standard to be followed:**

(1) Does the processing involve activities that relate so special PI?

(2) Will the processing of this information take place on a large scale?

- 'Large scale' if: many research participants are involved; or a large proportion of a population is involved; or a large volume of PI will be collected, or the processing will take place over a long period.

UNISA college of law

High-risk activities (cont.)

(3) Will the activities/processing involve the evaluation of PI to make automated decisions with legal consequences or which may have a substantial effect on the data subjects?

- This would include activities such as profiling and predictive analysis (for example, genetic testing) to make an automated decision about a data subject that will have a significant effect on him/her
- A decision is automated if there is no human involvement in the decision. For the answer to be 'Yes', the decision must affect the data subject's circumstances, behaviour, choices, financial status, health, reputation, access to services or other economic or social opportunities

High-risk activities (cont.)

(4) Will the processing involve PI not provided to the responsible party by the data subjects/patients themselves?

(5) Will the SPI be disclosed to third parties?

(6) Will any other party in another jurisdiction have access to this information?

(7) Will unique identifiers be used to link, combine or match PI from multiple sources?

- The answer here is YES when different sets of PI held by other organisations or persons are linked by using unique identifiers to form a new dataset.

High-risk activities (cont.)

(8) Does the activities involve the use of new/unusual technology seen by individuals as privacy intrusive, such as AI, machine learning, deep learning, smart or wearable technology, tracking technology or the use of biometric information?

(9) Would data subjects/research participants be surprised or uncomfortable to learn what their PI will be used for, or how it will be used?

(10) Will the activities involve the processing of information from individuals *in ways* they might find intrusive?

(11) Will it be difficult to obtain consent from or provide information to data subjects on how their Personal Information will be processed?

Practical example

- May PI that was obtained in the completion of previous research projects be used where consent to the re-use or sharing of personal information was not requested by donors? What if downstream commercialisation is an objective of the research?
  - Looking at 11 questions, at least 8 can be ticked, hence high-risk processing
  - Gap analysis should be done, & IO approve research protocol; relevant safeguards be put in place & compliance monitored every 2nd year

Practical example (cont.)

- Scientific outcomes, including commercial benefits that will follow, must be disclosed to participants
- Answer to previous slide's question – provided that:
- the participant's privacy will not be adversely affected to a disproportionate extent
- and that the data will not be published in an identifiable form,
- and security measures are place
- AND protocol was REC-approved,

The personal information can be re-used/shared under POPIA

Draft POPIA Code of Conduct for Research*

- POPIA applies whilst CoC still not approved yet
- RP must apply for prior authorisation if there is linking or transfer of special personal information (or unique identifiers) or the use of identifiers for other purposes; or the transfer of PI to third countries
- Information Regulator must be approached for prior authorisation before the activity commences or continues*
- Information Regulator needs to determine whether there are satisfactory safeguards in place to protect the personal information—security of information
- Prior authorisation requirement in force since 1 July 2021; was not necessary to suspend processing pending prior authorisation for research activities that started before 1 July 2021
- **This requirement has changed on 1 February 2022.** Research activities subject to prior authorisation **will have to be suspended pending prior authorisation**

* susan@assaf.org.za – presentation to NHREC 18/8/2022 (Dr S Veldman; Director/ASSAf)

UNISA college of law

Data access committees & data sharing

- POPIA: no guidance on Data Access & Transfer Committees
- No uniform ToR's; SoP's in SA
- DSI, DoH, SAMRC hosted seminar on establishing a DTA for health research in SA on 26 June 2022
- Align the Open Science drive, the Draft SA National Open Science policy & the 2021 the Draft National Data and Cloud policy with POPIA and the national MTA

Elements to consider in a DTA

6. Details of **planned sharing arrangements** with third parties.
7. If the data will **be shared on open access** platforms
8. The **security measures in place** to safeguard access to the data and prevent unauthorised access to the data, including how security breaches will be mitigated.
9. Who holds **intellectual property rights**, should the data generate results that are capable of intellectual property protections.
10. Whether there will be **any direct benefits to the provider or direct or indirect benefits to participants** or the participant community.
11. Whether the research **participants' consent is in line with the provisions set out in the DTA**.

UNISA college of law

Conclusion

- POPIA: complex, multi-layered, yet principles-based and no context specific
- Code of Conduct ito POPI (re processing of genetic/genomic information; sample & data storage & re-use; import & export of samples & data; limits to sample & data withdrawal)
- Clarity on consent model (DoH guidelines) for genetic research vis-à-vis POPIA and NHA
- REC training include training on data sharing & transfer; DTA and MTA