elsabé klinck associates pty ltd

The POPI Act and the sharing of personal information

@EKConsulting1

Conditions for *lawful* processing or as we call them 7 Cardinal Rules:

1. **"Accountability":** responsibility to ensure compliance
2. **"Processing limitation":** lawful (consent, law or "legitimate business interest"), minimal
3. **"Purpose specification":** purpose specific and explicitly defined (& consented to!)
4. "**Further processing limitation":** only if it formed part of the *originally*-obtained, explicit- and specifically consented to purpose of the processing. OR: necessary to prevent threat to public health or safety or the life or health
5. **"Information quality":** responsible party to take steps to ensure info is complete, accurate, not misleading and updated
6. **"Openness":** notifying data subjects, such as if the data-collection is mandatory or voluntary), and the circumstances in which such compliance would not be necessary (viz. where the data subject has consented or where a law authorises the processing)
7. "**Security safeguards":** list of measures that should be taken to prevent loss, damage, unauthorised and unlawful access

ek &a

POPI: Special information (health and biometric)

- Processing of this information is, in general, **prohibited**, unless **consent** has been provided; the data is necessary to exercise a right or fulfill a legal obligation; and sufficient guarantees for indiv.
- Section 32 excludes from the prohibition: medical professionals and healthcare facilities, insurance companies and medical schemes/administrators deal with authorisations relating to health, but requires that information only be processed under a contractual duty of confidentiality, unless there is a legal duty to process the information

ek
&a

Main responsible party

- Hospital record contains personal information of patient, the hospital and also proprietary information of the hospital

- Medical device companies not listed in section 32, POPIA, therefore need consent from entities whose information would be processed

Therefore,

- Consent…patient
  - Directly from the patient (or incapacitated, next of kin / mandated person)
  - Must declare that there because of consent to specific treatment provided to the treating practitioner (keep record of written referral)
  - Comply with all 7 conditions of processing
  - Declare if for funding and/or treatment
- Consent of hospital
- Staff / contractor:
  - Policy and included in contracts
  - In some instances Operator Agreement is necessary with third parties doing submissions to RAF, for example

elsabé klinck associates pty ltd

QUESTIONS IR MAY ASK…

@EKConsulting1

The Covid database… IR queries NDOH

- Compliance with all 8 conditions (incl the de-identification on the Tracing Database).
- DoH had to report to it by 29 April 2022, on how it and/or NICD -
  - will comply with applicable conditions for lawful processing of personal information.
  - measures taken or to be undertaken to ensure compliance with the de-identification requirements,
  - the retention period for personal information collected for track-and-trace purposes,
  - the method or manner to be applied in destroying or deleting the records of personal information.
- Whether the DoH or NICD intends to transfer to a third party who is in a foreign country and the level of protection afforded by the foreign country.
- Details about the nature or category of the special personal information and personal information of children held by, or under the control of, these institutions

https://inforegulator.org.za/wp-content/uploads/2020/07/Final-MEDIA-STATEMENT-INFORMATION-REGULATOR-MONITORS-THE-DEPARTMENT-OF-HEALTHS-POPIA-COMPLIANCE-22-APRIL-2022.pdf

ek &a

Enforcement Notice: Dischem

The Regulator's assessment found that Dis-Chem failed to:

- identify the risk of using weak passwords and prevent the usage of such passwords.
- put in place adequate measures to monitor and detect unlawful access to their environment.
- enter into an operator agreement with Grapevine and ensure that Grapevine has adequate security measures in place to secure personal information in its possession. Furthermore, the agreement would have outlined processes of
in the event of a security compromise.

- conduct a Personal Information Impact Assessment to ensure that adequate measures and standards exist to comply with the conditions for the lawful processing of personal information as required by Regulation 4(1)(b) of POPIA.
- implement an adequate Incident Response Plan. implement the Payment Card Industry Data Security Standards (PCIDSS) by maintaining a vulnerability management programme, implement strong access control measures and maintain an Information Security Policy.
- ensure that it concludes written contracts with all operators who process personal information on its behalf, and that such contracts compel the operator(s) to establish and maintain same or better security measures referred to in section 19 of POPIA.
- develop, implement, monitor, and maintain a compliance framework, in terms of Regulation 4(1)(a) of POPIA which clearly makes provision for the reporting obligations of Dis-Chem and all its operators in terms of section 22 of POPIA.

- No personal info impact assessment done
- No operator agreement
- Weak passwords
- No PCIDSS implementation

elsabé klinck associates pty ltd

Thank you!

elsabe@elsabeklinckassociates.co.za

@EKConsulting1