elsabé klinck associates pty ltd

POPI

What Medtech companies need to know - Protection of patient information

@EKConsulting1

POPI

(protection of information)

POPI restricts access to personal information in terms of information in terms of s 14 of the Constitution

VS.

PAIA

(access to information)

PAIA promotes access to information in terms of section 32(1)(a) of the Constitution

Discussion Points

1. Important Concepts
2. Conditions of Lawful Processing PI
3. Patient Information – What to do
4. Queries - FAQ
5. Practical Implementation
6. Risk Assessment
7. Security Measures
8. Industry Code

Important Concepts

WHAT IS A DATA SUBJECT?

The Person to whom the personal information relates to

- natural or juristic

(e.g. Customers, patients, service providers, vendors, employees, hospitals, manufacturers, logistics)

RESPONSIBLE PARTY?

- Person who determines what the purpose for the processing of personal information will be

INFORMATION REGULATOR?

- Juristic body established in terms of POPIA to see that there is compliance with both the Act and Promotion of Access to Information Act (PAIA)

OPERATOR?

Person who processes PI for or on behalf of a responsible party i.t.o a contract, mandate ***without coming under the direct authority of that party***

E.g.

- Security (CCTV, etc.)
- Brokers
- Payroll
- Others???

International Operators

(e.g. databases hosted via Google or Amazon or …)

- **YOU: Remain responsible** – **not the Operator** **Except S 106: Account number third party is liable if aware**
- **Cross Border Transfer of information (by vendors or Operators)**
  - Data Subject Consent and
  - Law in the other country or
  - Agreement or
  - Binding Corporate rules

  That are substantially similar to the principles of the 8 conditions of lawful processing under POPI

Conditions of lawful Processing

CONDITIONS OF LAWFUL PROCESSING

1. **“Accountability”:** responsibility to ensure compliance

2. **“Processing limitation”:** lawful, not excessive, consent, legal obligation,

3. **“Purpose specification”:** purpose specific and explicitly defined (and consented to!).

4. **“Further processing limitation”:** only if it formed part of the *originally*-obtained,

5. **“Information quality”:** responsible party to take steps to ensure info is complete, accurate, not misleading and updated

CONDITIONS OF LAWFUL PROCESSING

6. **“Openness”:** notifying data subjects - is the data-collection is mandatory or voluntary
7. **“Security safeguards”:** list of measures that should be taken to prevent loss, damage, unauthorised and unlawful access.
8. **“Data Subject Participation”:** Right to request a record about them, who their information was shared with

Patient Information

PATIENT INFORMATION

1. **Do not collect patient information unless you have to!!** Condition 2 & 3 – Limitation & Purpose: lawful, not excessive, consent, contract, legal obligation.
    - **Adverse Events:**
        - Does the law require the patient information?
        - SAHPRA requires only initials, gender, DOB/Age – NO FULL NAMES!!
    - **Traceability:**
        - Does the ISO/Law require patient information OR- ***Unique identification must be given to the device***

2. Invoicing

- Consignment
- Device order

QUERIES

QUESTIONS

1. Passwords for opening documents?
   - It is not a POPI requirement, what is reasonable?
2. Training – **Reg 4 Requirement**
3. Authorisations on behalf of surgeons, Patient implant queries, Pt detail on invoicing, all patient data on report analyses
   - Anonymise patient information/identity/use file number/identifying code
4. Registration of Information Officer – **NO DEADLINE**

REGISTRATION OF INFORMATION OFFICERS PORTAL
*Please note we are experiencing technical issues with the Portal, which results in it not being accessible at the moment. Our technicians are working on it. The Portal will be **accessible** as soon as these issues are resolved. We apologise for the inconvenience caused.*

5. How other companies are doing it?

- Industry Code can be developed to assist.

6. Liability of Deputy Information Officers

- As an employee

QUESTIONS

7. Use of patient information on invoices- password protection of invoices?

8. Mediclinic is no longer sharing patient information:

- How to handle traceability? ISO 13485
- How to deal with AE?

9. Marketing

- Get consent to market, provide opt out options!

10. New Policies /SOP's/Privacy Notices – **Condition 6**

11. Why the bullying?

- Know the law, what services are you providing, are you a vendor or operator?

12. We need the industry hospital groups , HCPs , Payers and Suppliers to unite and work on a plan that will still ensure compliance to POPI while meeting patient needs and attending regulatory requirements.

QUESTIONS

13. Assume that everything is personal information?

- *“includes”* or *“not limited to”*

14. Practical Implementation/ Portal not working/No responses from Information Regulator

Practical Implementations examples

- Register with Information Officer and Deputy with the Information Regulator
- Get training on Information Officer duties
- Development and implementation of a **Compliance Framework**;
  - PAIA Manual and
  - POPI Policy
- Perform and record **personal information impact assessment** (including risks on security)
- Perform **security assessment internal measures and adequate systems** to process PI
- Implement **adequate security measures**
- Implement **standards to comply with the conditions for the lawful processing**;
- **Process and record requests for information and other data subject rights**; and
- **Internal awareness** sessions should be conducted regularly – **Regulation 4 of POPI**
- Report and notify Information Regulator and Data subject of breach or suspected breach
- **Main contact with the Information Regulator** during investigations and inspections

RISK ASSESSMENT

Risk Assessment

Doing a risk assessment is a requirement:

- Identifying Special Information - in the Act
- Identifying the risks associated with other information, e.g. financial information.
- Ask: *what is the impact of breach on the Data Subject and the Business? Is it High, Medium, Low?*
- Determine what security measures must be put in place depending on the category information, or one measure of security for all? (the most stringent one for all?? Costs??)

ek
&a

Risk Assessment and Review

- **NOT** once off!
- POPI **requires** you to **regularly** do an assessment of how you process Personal Information against the **8 conditions**.
- Do a security risk assessment regularly: E.g.
  - How safe are my **surroundings** – physical break-ins and breaches, any changes since the last assessment??
  - **Internal** assessment? Employee loss of devices, erroneous deletion
  - How safe are my **IT protections**?? Any changes since the last report?
  - **What is the industry doing**? What is acceptable?
  - Do a self-audit. i.e. pick out a sample of random contracts/clients and assess whether or not the requisite conditions have been complied with.

For small entities, this may be an easy exercise, but for larger companies…???

Security Measures

POPI Requirements in the PAIA Manual

Security Measures

19. *(1) A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent—*

- *(a) loss of, damage to or unauthorised destruction of personal information; and*
- *(b) unlawful access to or processing of personal information.*

INDUSTRY CODE

Industry Code – Section 62

The Information Regulator encourages Industries to develop Codes of Conduct that will assist members to comply with POPI

(2) A code of conduct must—

(a) incorporate all the conditions for the lawful processing of personal information or set out obligations that provide a functional equivalent of all the obligations set out in those conditions; and

(b) ***prescribe how the conditions for the lawful processing of personal information are to be applied, or are to be complied with****, given the particular features of the sector or sectors of society in which the relevant responsible parties are operating.*

(3) A code of conduct may apply in relation to any one or more of the following—

…

(4) A code of conduct must also—

(a) ***specify appropriate measures—***
(i) for information matching programmes if such programmes are used within a specific sector; or

(ii) for protecting the legitimate interests of data subjects insofar as automated decision making, as referred to in section 71, is concerned;

…

& elsabé klinck
associates pty ltd

pat@elsabeklinckassociates.co.za

@EKConsulting1