PoPI Compliance through Access Control of Electronic Health Records

Tamir Tsegaye

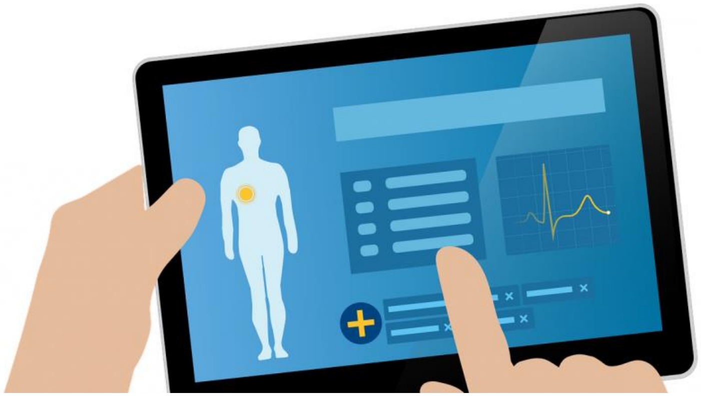
Stephen Flowerday

Outline

- Background
- Research problem
- Research methods
- Comparison of regulations with PoPI Act principles
- Characteristics of regulations
- Security and privacy standards for aiding compliance
- Proposed model for assisting compliance
- Future research
- Conclusion

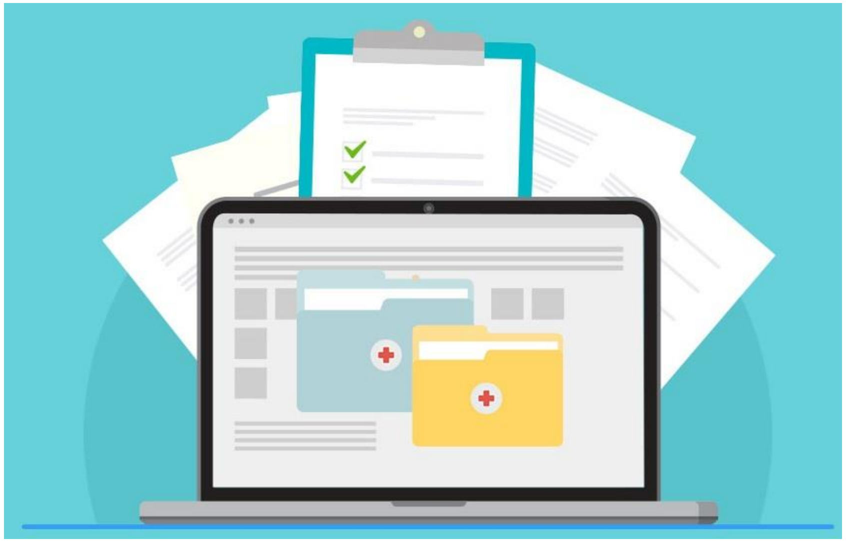
Background

- Electronic health record (EHR) aims to improve healthcare delivery by providing clinicians with access to patients’ complete medical history.
- South Africa has attempted to adopt EHR in national context through implementation of national EHR system.



Background

- National EHR system forms part of South Africa’s National Health Insurance (NHI) strategy.
- NHI focuses on improving accessibility of health services to all South Africans.



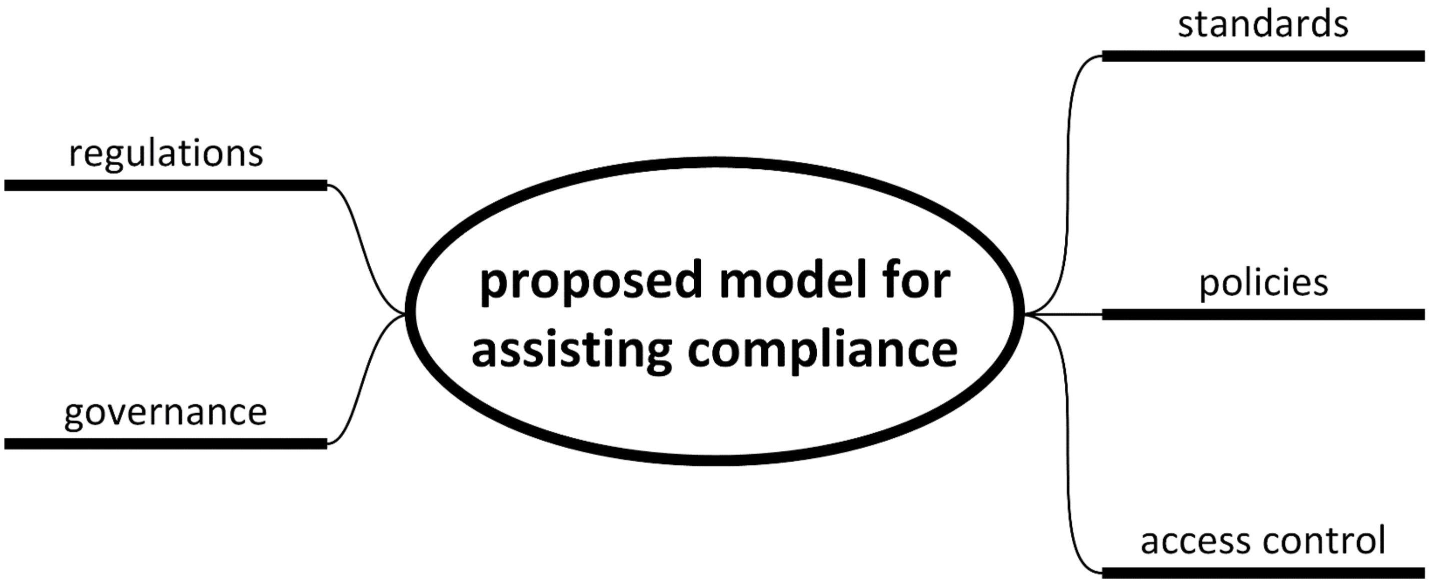
Research Problem

- Patients’ EHRs at risk of unauthorised access or misuse by authorised clinicians: accessible nationally.
- Regulations such as Protection of Personal Information (PoPI) Act mention that personal information must be protected.
- However, do not indicate what processes must be followed in order to ensure compliance.
- **Contribution of study:** proposed model indicating components needed to support compliance through enforcement of access control for securing the EHR.

Research Methods

- Scoping review – based on five stages of Arksey and O’Malley’s framework:
    1. Identifying research question: *What processes should be followed to assist compliance with regulations in order to protect patients' EHRs?*
    2. Identifying relevant studies
    3. Study selection
    4. Charting data
    5. Collating, summarising and reporting results
- Thematic analysis:
    - ➢ Recorded codes identified as themes informing proposed model.
    - ➢ Themes included in proposed model as components.

Themes Informing Proposed Model



Comparison of Regulations with PoPI Act Principles

- PoPI Act basis for comparison since it is most relevant regulation for protecting EHR.
- Convergence exists between eight PoPI Act principles and examined regulations.
- Majority of examined regulations (Directive 95/46/EC, DPA, GDPR, PIPEDA and the Privacy Act) based on data protection principles similar to PoPI Act principles.
- Although HIPAA and PDA regulations do not contain sections outlining data protection principles, content overlaps with PoPI Act principles.

Comparison of Regulations with PoPI Act Principles

PoPI Act (South Africa) Principles	Description	Directive 95/46/EC (EU)	DPA (UK)	GDPR (EU)	HIPAA (US)	PDA (Sweden)	PIPEDA (Canada)	Privacy Act (New Zealand)
Accountability	Eight principles for lawful processing of personal information must be complied with	✓	✓	✓	✓	✓	✓	✓
Processing limitation	Limits must be placed on the processing of personal information	✓	✓	✓	✓	✓	✓	✓
Purpose specification	Collection of personal information must be done for a specific and lawful purpose	✓	✓	✓	✓	✓	✓	✓
Further processing limitation	Further processing of personal information must be compatible with original purpose for which information was collected	✓	✓	✓	✓	✓	✓	✓
Information quality	Collected personal information must be complete, accurate, not misleading and up to date	✓	✓	✓	✓	✓	✓	✓
Openness	Responsible party must be open by notifying Information Regulator before processing personal information. Subject must also be notified about processing	✓	✓	✓	✓	✓	✓	✓
Security safeguards	Confidentiality and integrity of personal information must be ensured through technical and organisational controls	✓	✓	✓	✓	✓	✓	✓
Data subject participation	Subject has the right to request their personal information, which is held by responsible party, as well as its correction	✓	✓	✓	✓	✓	✓	✓

Characteristics of Regulations

- Characteristics of regulations relevant for regulating processing of personal information in national EHR system:
  - Processing
  - Security
  - Data protection authority
  - Data breach notification
  - Enforcement
  - Data protection officer

Characteristics of Regulations

Characteristic	Directive 95/46/EC (EU)	DPA (UK)	GDPR (EU)	HIPAA (US)	PDA (Sweden)	PIPEDA (Canada)	PoPI Act (South Africa)	Privacy Act (New Zealand)
Processing	✓	✓	✓	✓	✓	✓	✓	✓
Security	✓	✓	✓	✓	✓	✓	✓	✓
Data protection authority	✓	✓	✓	✓	✓	✓	✓	✓
Data breach notification		✓	✓	✓		✓	✓	
Enforcement	✓	✓	✓	✓	✓	✓	✓	✓
Data protection officer		✓	✓	✓		✓	✓	✓

Security and Privacy Standards for Aiding Compliance

- ISO 29100:
  - Provides privacy framework for protecting personal information stored in systems.
  - Focuses on processing of personal information: aligned with examined regulations.
- ISO 27001:
  - Indicates requirements for assessing and treating information security risks specific to organisation through implementation of information security management system.
- Both standards support privacy by design.

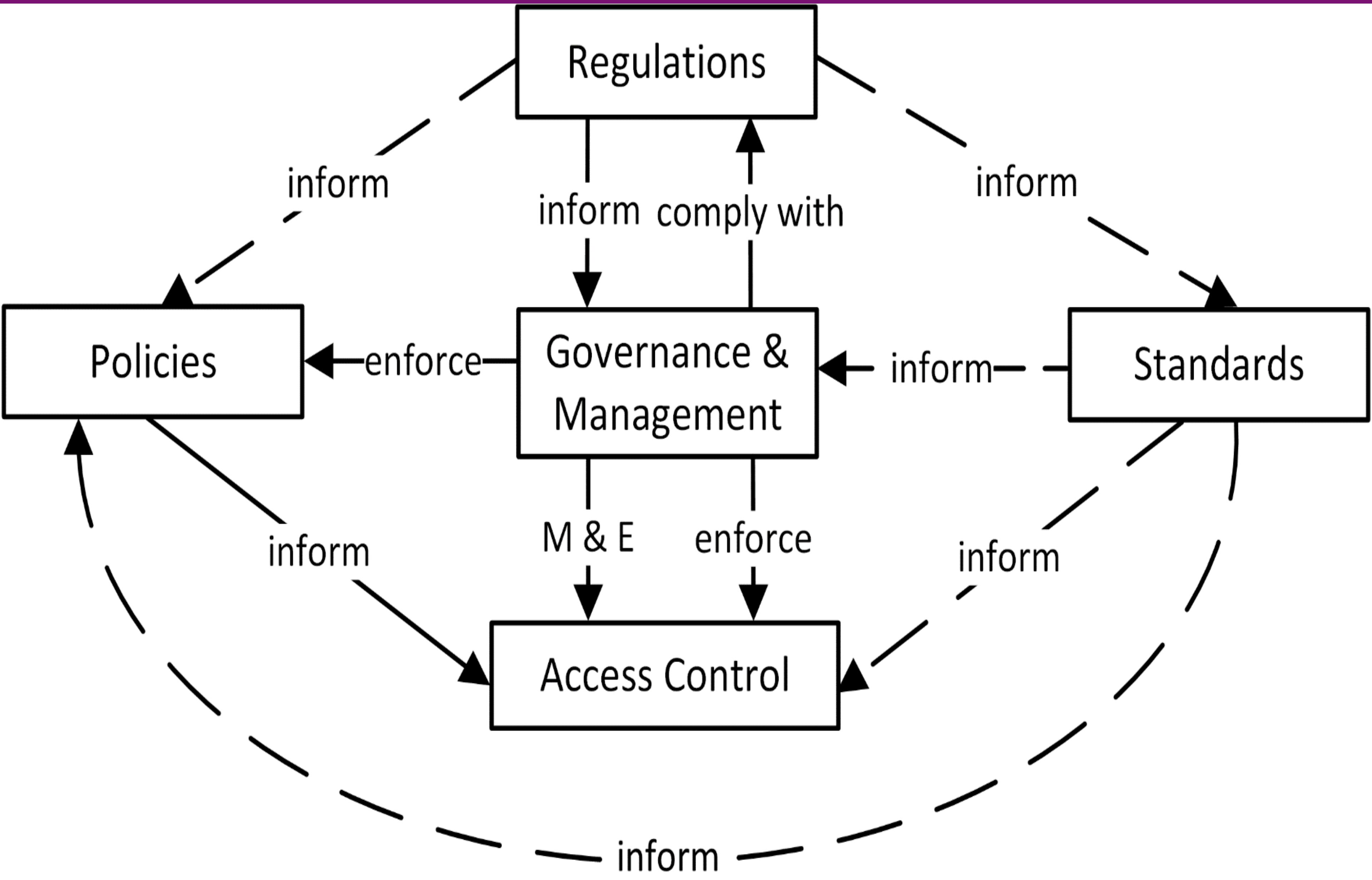
ISO 29100 to PoPI Act Mappings

ISO/IEC 29100 Privacy Principles	PoPI Act Principles
Consent and choice	Processing limitation
Purpose legitimacy and specification	Purpose specification
Collection limitation	Processing limitation
Data minimisation	Processing limitation
Use, retention and disclosure limitation	Further processing limitation
Accuracy and quality	Information quality
Openness, transparency and notice	Openness
Individual participation and access	Data subject participation
Accountability	Accountability
Information security	Security safeguards
Privacy compliance	Accountability

ISO 27001 Control Areas for Access Control

Section	Control Area
A.5	**Information security policies**
A.6	Organisation of information security (A.6.1.2 **Separation of duties**)
A.9	**Access control**
A.12	Operations security (A.12.4 **Logging and monitoring**)
A.18	**Compliance**

Proposed Model for Assisting Compliance

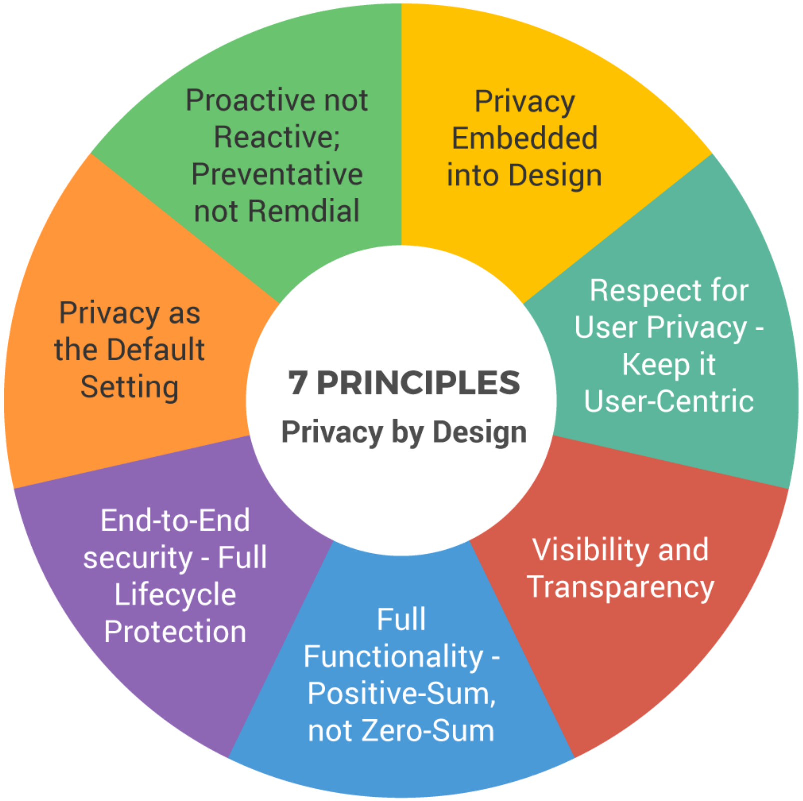


Proposed Model: Overview

- **Regulations**: influence operation of access control through other components.
- **Governance and management**: comply with regulations e.g. PoPI Act by enforcing policies and access control.
- **Policies**: inform operation of access control.
- **Standards**: inform both policies and access control.
- **Access control**: prevents unauthorised disclosure and modification of EHR – using role-based access control and attribute-based access control.
- **M & E**: maintaining compliance with PoPI Act.

Future Research

- Investigating privacy by design in more detail in terms of how it may be leveraged to aid PoPI compliance.


Proactive not Reactive; Preventative not Remdial
Privacy Embedded into Design
Respect for User Privacy - Keep it User-Centric
Visibility and Transparency
Full Functionality - Positive-Sum, not Zero-Sum
End-to-End security - Full Lifecycle Protection
Privacy as the Default Setting
7 PRINCIPLES
Privacy by Design

Conclusion

- South Africa aims to implement national EHR system in order to improve healthcare delivery.
- EHRs at risk of unauthorised access or misuse by authorised clinicians.
- PoPI Act compared with other countries' regulations indicating convergence.
- Characteristics of regulations relevant to regulation of national EHR system.
- ISO 29100 and 27001 for aiding compliance both support privacy by design.
- Proposed model indicated components for assisting compliance: secure EHR through enforcement access control.
- All references included in published paper.

Questions