RHODES UNIVERSITY
Where leaders learn

An Access Control Model for a South African National Electronic Health Record System

Tamir Tsegaye

Masters of Commerce Research Project

Supervisor: Prof Stephen Flowerday

Co-supervisor: Prof Graham Wright

Outline

- Background
- EMR vs EHR
- Proposed Access Control Model
- Proposed Model: Contributions
- Retrieval of National EHR at Region A
- Retrieval of National EHR at Regions B, C and X
- National EHR: Access Control
- National EHR: Regulations
- National EHR: Interoperability
- Theoretical Foundation

Background

- National Health Insurance (NHI): focuses on improving accessibility of health services to all South Africans.
- NHI includes implementation of interoperable national Electronic Health Record (EHR) system.
- The national EHR system critical enabling factor for implementation of NHI.

Background

- **Research problem:**
  - complexity involved in balancing requirements of security, privacy and access of EHR.
  - security and privacy of patients' EHRs at risk due to sharing of EHRs with increasing number of parties.
- **Objective of study**: develop access control model that will address research problem.
- **Contribution of study**: proposed model that indicates how EHR secured using access control and how interoperable national EHR can be realised.
- Proposed model evaluated via expert review.

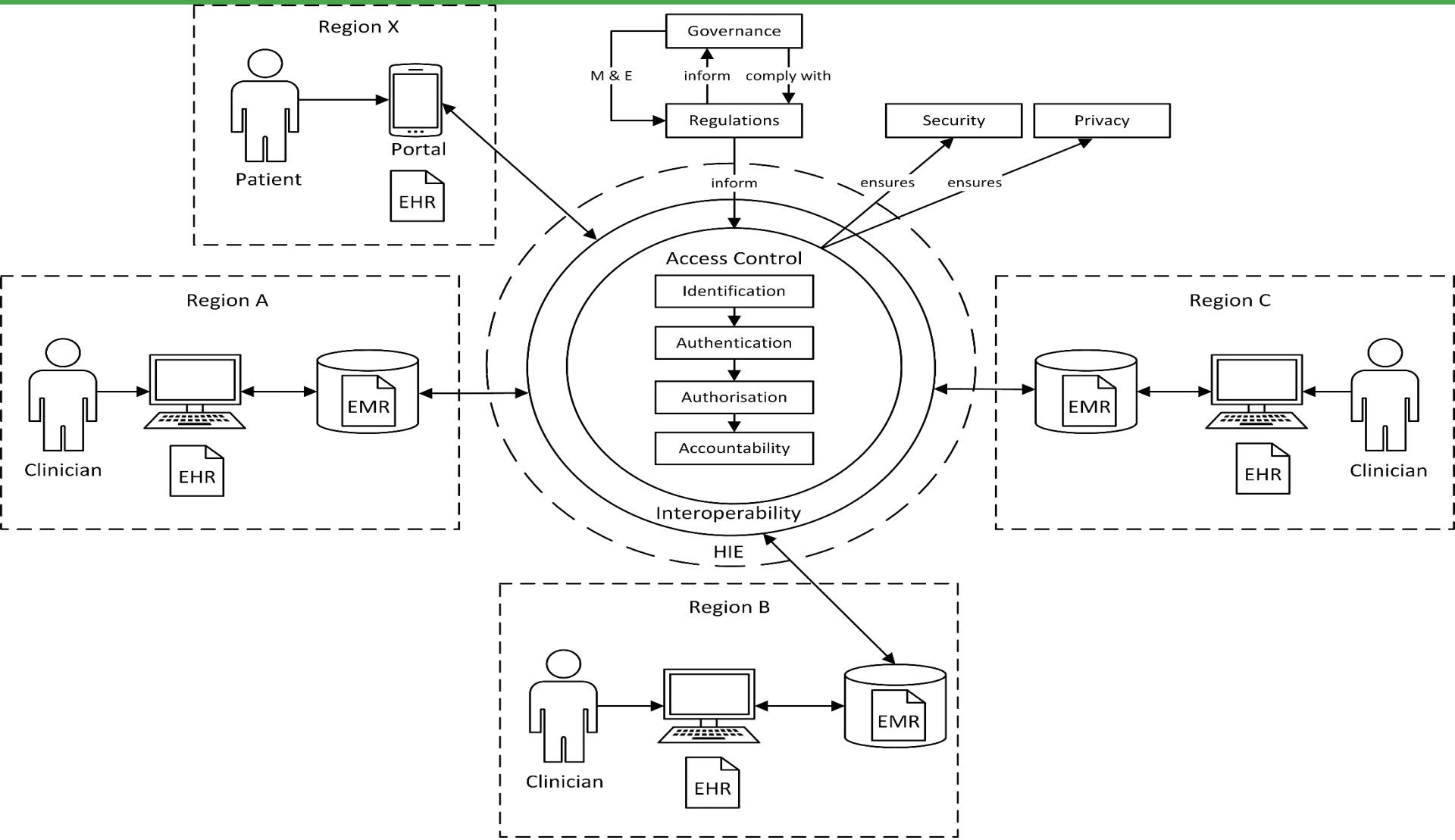
Background

- Creation of proposed model:
  - Content analysis method conducted using MAXQDA software programme on literature sample in area of access control and EHR.
  - Literature sample read and key terms tagged as codes: initially 228 codes.
  - Codes reduced to 12 codes, which informed proposed model.

EMR vs EHR

- Below definitions discussed and illustrated in proposed model:
  - **Electronic Medical Record (EMR)**: electronic record of patient encounter within single health facility (CSIR & Department of Health, 2014).
  - **Electronic Health Record (EHR)**: longitudinal electronic record of patient's information consisting of one or more encounters in any health facility (Deloitte, 2015).

Proposed Access Control Model



Proposed Model: Contributions

- National EHR system architectures of 5 countries examined in literature: Canada, New Zealand, South Africa, Sweden and England (Canada Health Infoway, 2006; CSIR & Department of Health, 2014; Deloitte, 2015; House of Commons, 2007; Sellberg & Eltes, 2017).
- Proposed model contributions:
  - IAAA (Identification, Authentication, Authorisation and Accountability) shows components of access control needed to protect national EHR.
  - Available access control models from literature do not illustrate use of IAAA for protecting national EHR.
  - Proposed model indicates how disparate EMRs aggregated to form national EHR.
  - Relationship between regulations and access control indicates how access control informed by regulations.

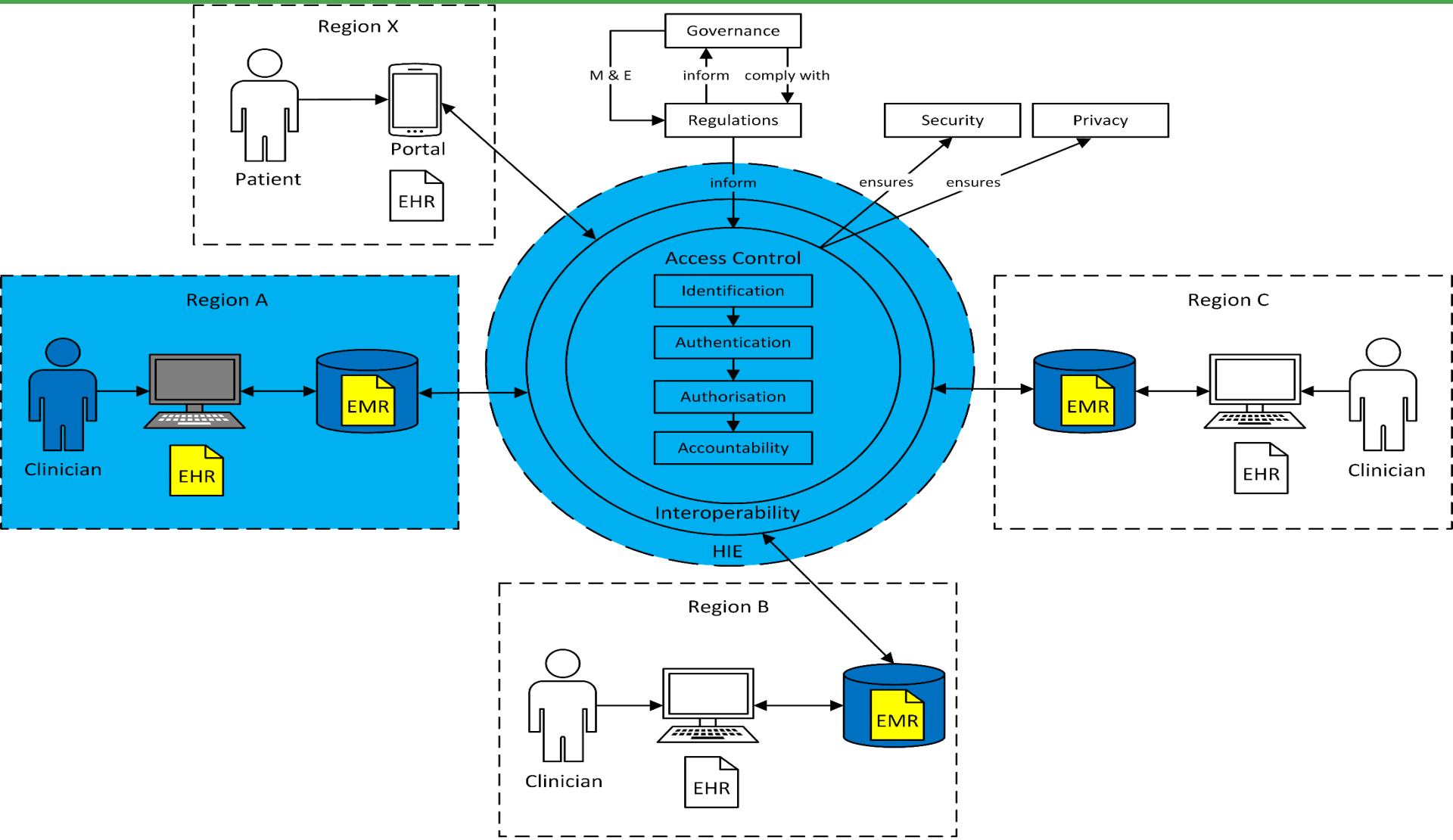
Retrieval of National EHR at Region A

- **Case 1:**
  - Patient admitted to hospital in Region A.
  - Patient previously visited this hospital and two other health facilities in Regions B and C.
  - Patient's encounters at these health facilities recorded in EMRs.

Retrieval of National EHR at Region A

- **Case 1 (cont.):** Doctor in Region A retrieves patient's EHR using distributed architecture:
  - Doctor authenticates in order to access patient's EHR.
  - Links to patient's EMRs stored in central system.
  - Central system queries health facilities which store patient's EMRs.
  - Central system returns patient's aggregated EHR: comprises of retrieved patient's EMRs located in Regions A, B and C.

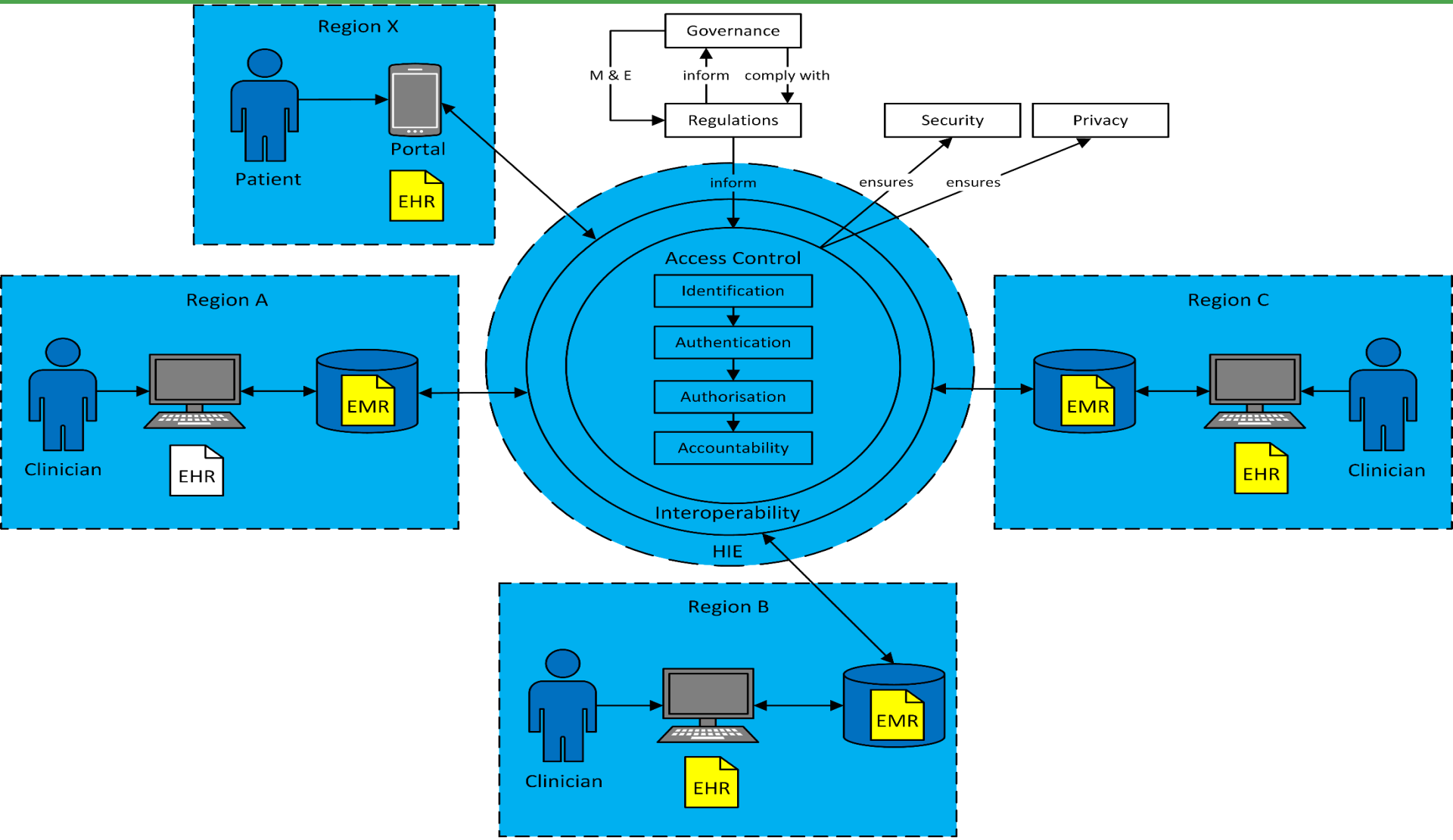
Retrieval of National EHR at Region A



Retrieval of National EHR at Regions B, C and X

- **Case 2:**
  - Doctor adds new health information to patient's EMR locally stored in hospital in Region A.
  - Updated EMR accessible, via distributed architecture, to authorised clinicians in other regions.
  - EHR also accessible to patient via web portal, accessible in Region X (any region in South Africa).

Retrieval of National EHR at Regions B, C and X



National EHR: Access Control

- Before clinician can access EHR, first three components of IAAA must be executed.
- Once executed, aggregated EHR returned by central system that contains patient information based on clinician's authorisation level.
- Fourth component of IAAA: Accountability executed regardless if clinician successfully authenticated or not.
- Use of access control ensures patient privacy and security.

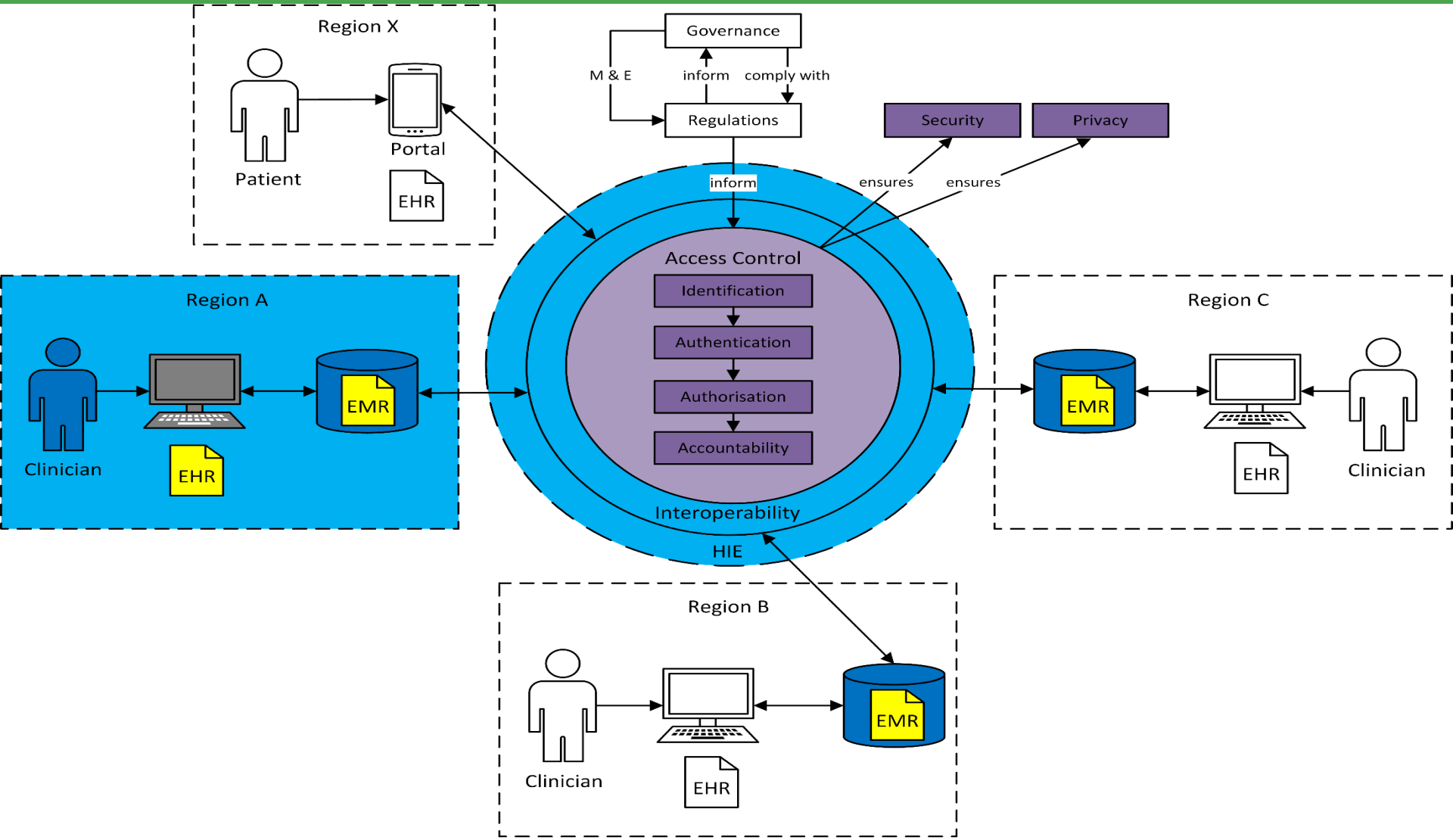
National EHR: Access Control

- **Case 3:** Nurse in Region A retrieves patient's EHR (patient's EMRs located in Regions B and C):
  - **Identification**: nurse identifies themselves using their username.
  - **Authentication**: nurse's identity checked by verifying credentials using two-factor authentication: single sign-on and smart card.
  - **Authorisation**: nurse granted access to EHR based on their role (role-based access control).
  - **Accountability**: access to patient's EHR logged including nurse's details, operations made (e.g. read), what information has been accessed etc.

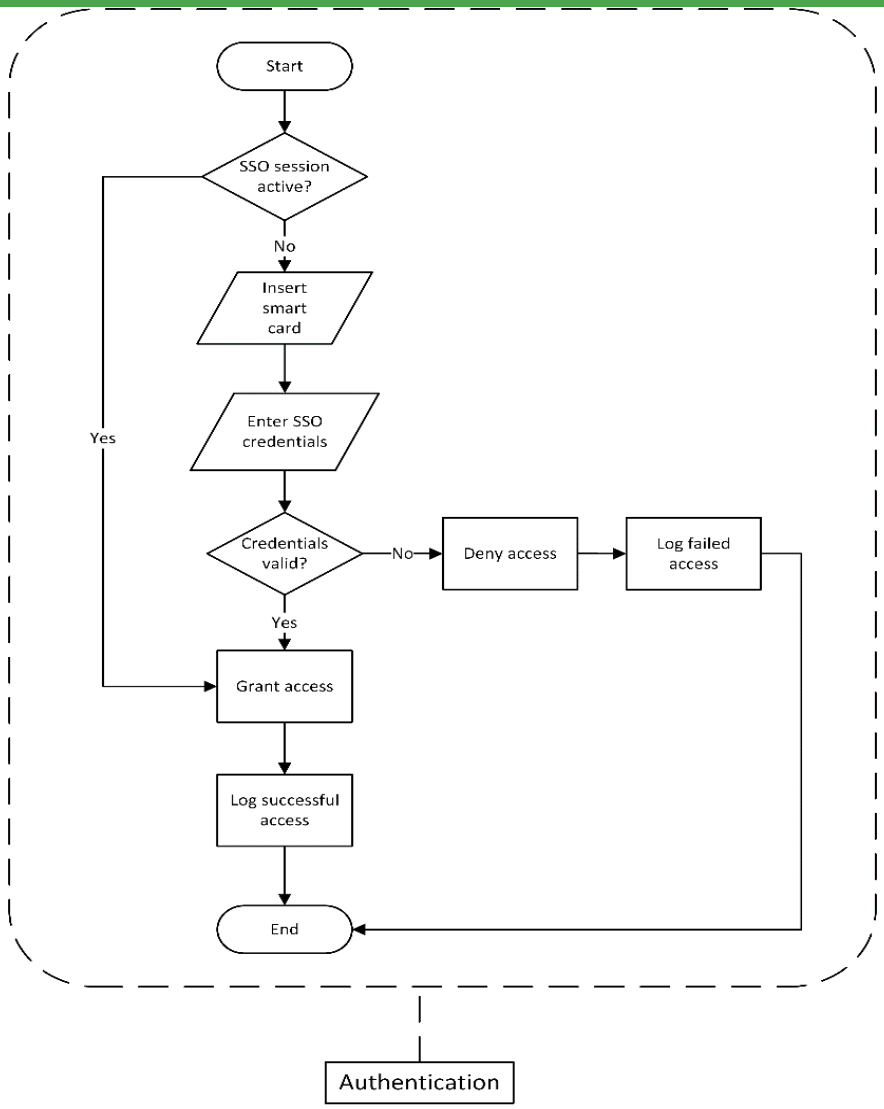
National EHR: Access Control

- Clinicians and patients authenticated using two-factor authentication:
  - Clinicians authenticate using single sign-on and smart card (granted read and write access to EHR).
  - Patients authenticate using single sign-on and one-time password via mobile app (only granted read access to EHR).
- Unlike clinicians, patients use one-time password instead of smart card since patient's would need to obtain smart card reader in order to authenticate.

National EHR: Access Control



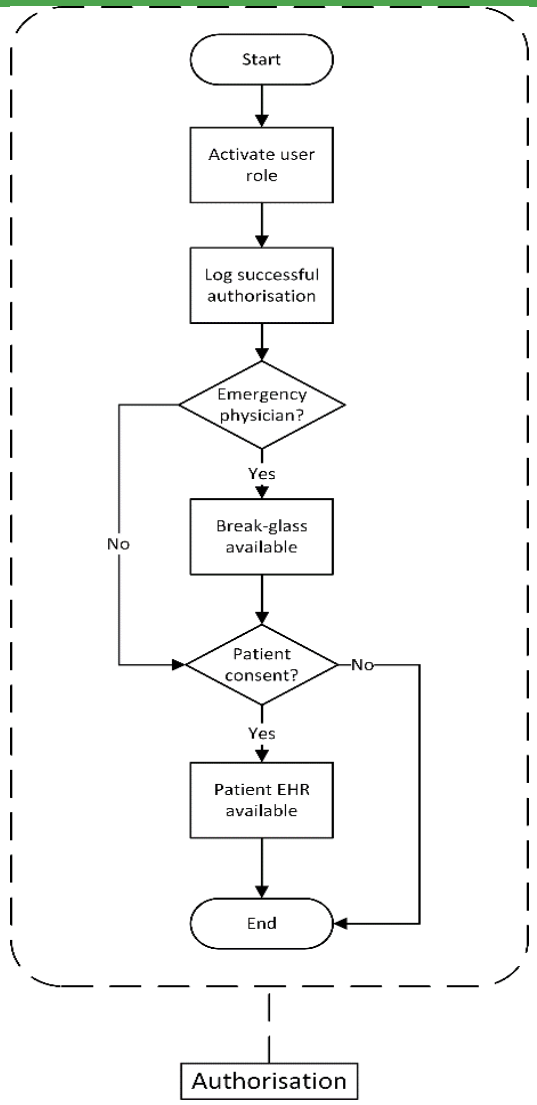
Clinician Two-Factor Authentication



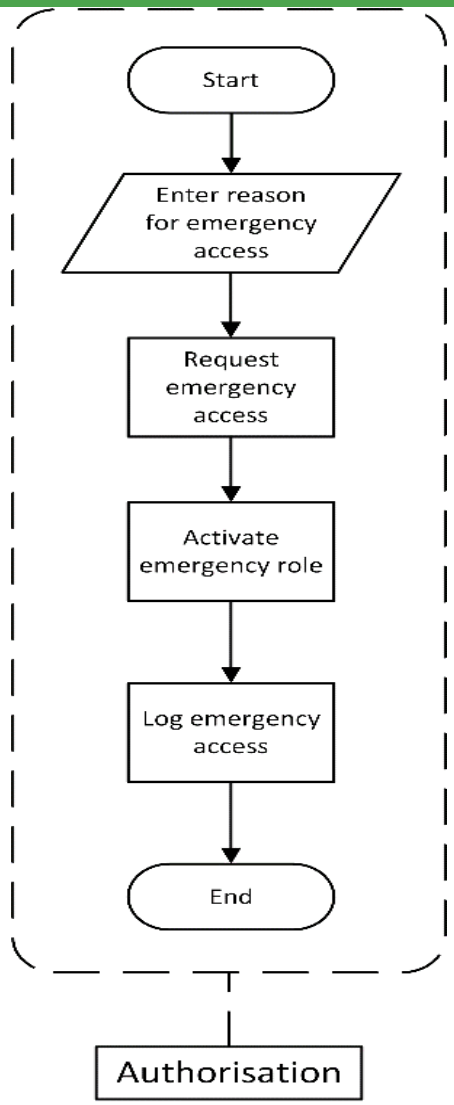
National EHR: Access Control

- Proposed model uses combination of Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) for making access control decisions:
  - RBAC: access to certain information granted based on user's role.
  - ABAC: uses attributes of users and objects in order to make access control decisions based on context e.g. medical emergency.

Clinician Authorisation Using RBAC & ABAC



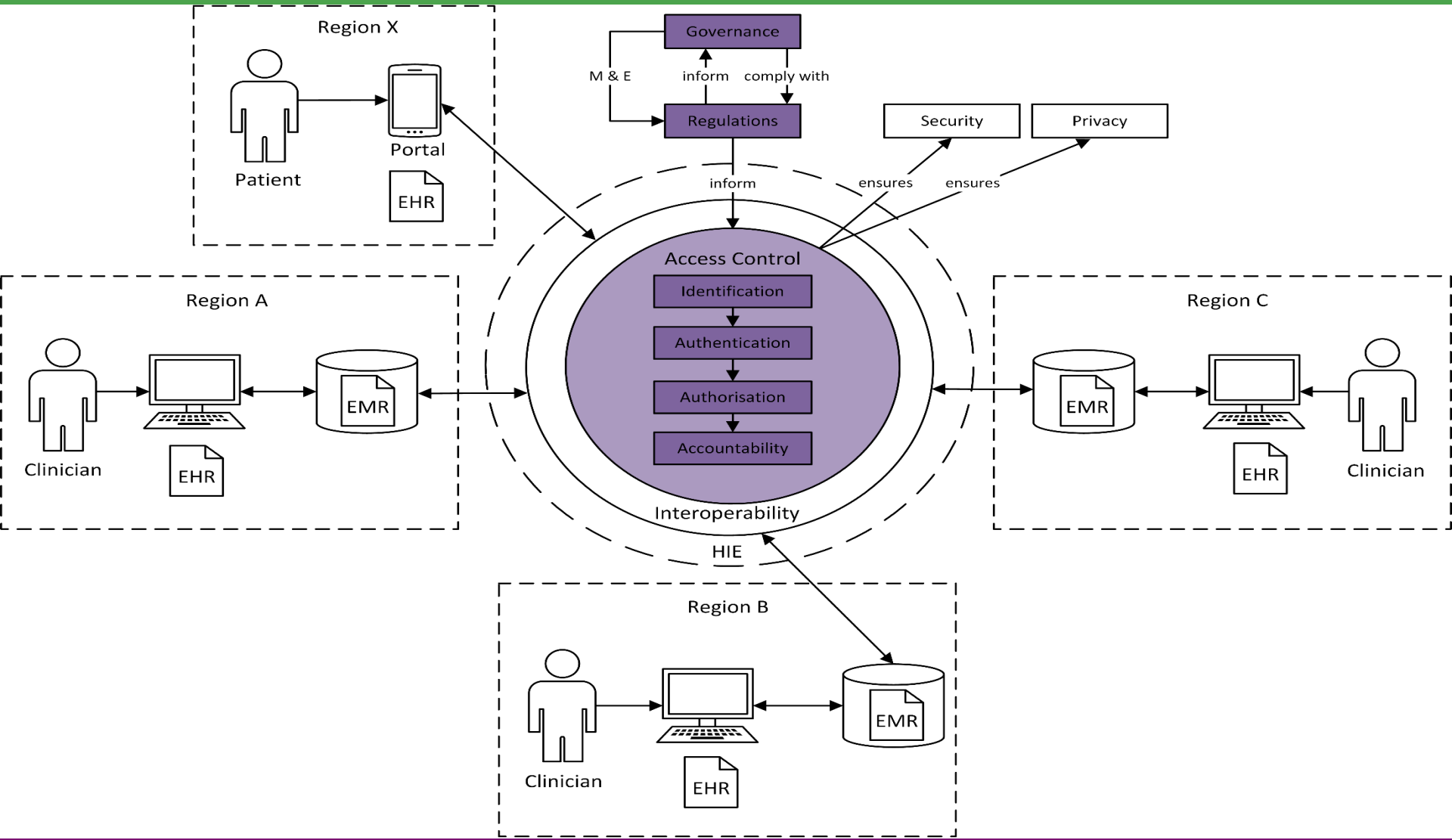
Clinician Requesting Emergency Access



National EHR: Regulations

- Access control informed by regulations:
  - Regulations aim to protect personal information.
  - Access control ensures protection by limiting disclosure of personal information to authorised entities.
  - Regulations inform governance which must comply with regulations.
  - Governance should periodically monitor and evaluate compliance with regulations.
  - PoPI (Protection of Personal Information) Act: most relevant regulation for protecting patient information.

National EHR: Regulations



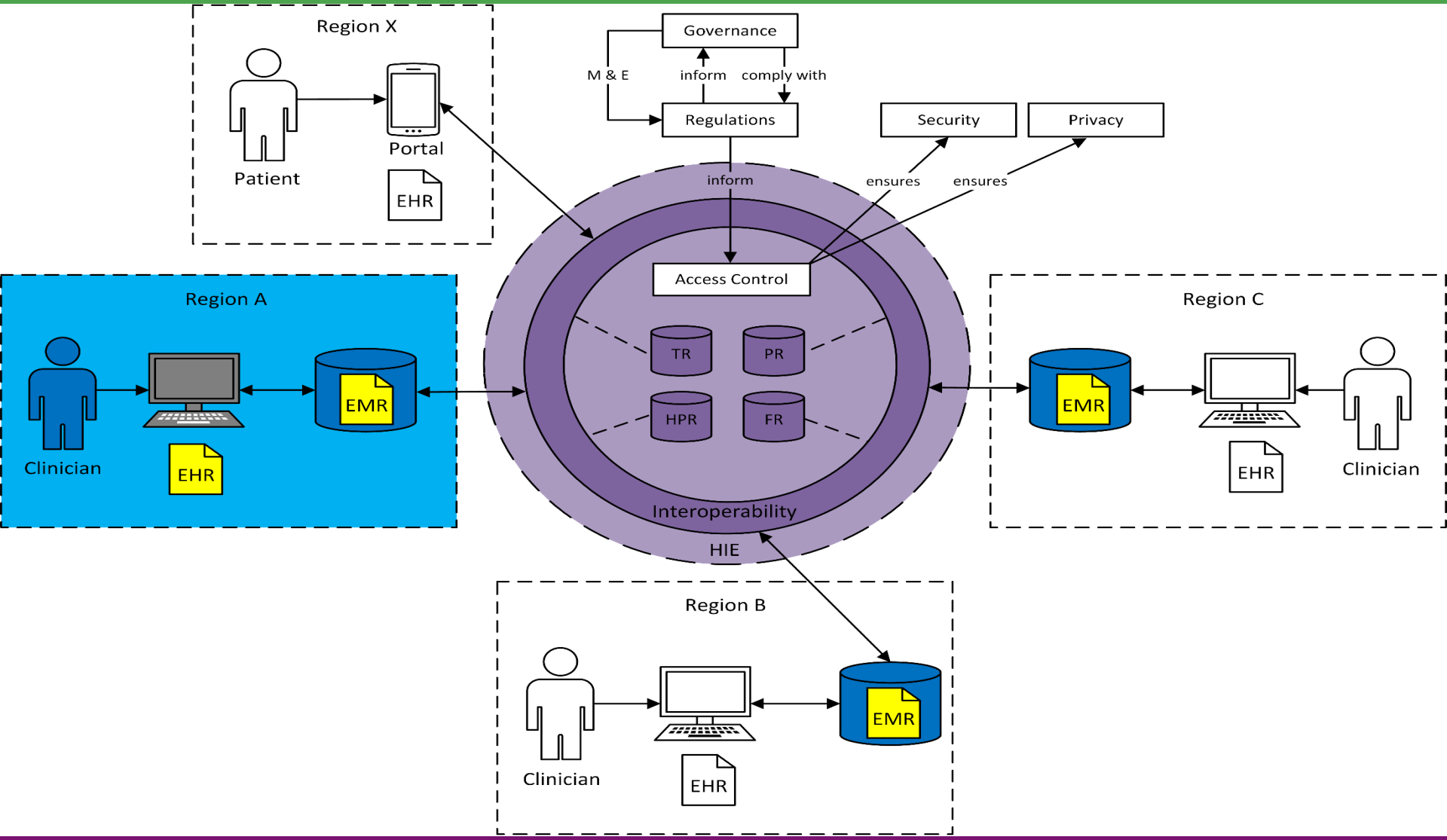
National EHR: Interoperability

- After first three components of IAAA executed, central system begins process of retrieving aggregated EHR.
- Central system's interoperability layer addresses all three levels of interoperability:
  - Foundational interoperability
  - Syntactic interoperability
  - Semantic interoperability

National EHR: Interoperability

- Interoperability layer aggregates disparate EMRs using common standardised format.
- Interoperability layer enables Health Information Exchange (HIE): allows exchange of EMRs between health facilities located in different regions.
- Registries play important role in HIE e.g. patient registry i.e. Patient Master Index.

National EHR: Interoperability



Theoretical Foundation: ANSI RBAC

- Study based on ANSI RBAC (Role-based Access Control) standards:
  - **ANSI INCITS 359-2012**: provides standardised definition of RBAC and its components.
  - **ANSI INCITS 494-2012**: extends ANSI INCITS 359-2012 by enabling RBAC standard to handle dynamic events e.g. medical emergency via ABAC (Attributed-based Access Control).
- Proposed model uses combination of RBAC and ABAC for making access control decisions.

Theoretical Foundation: Clark-Wilson

- **Clark-Wilson model** addresses goals of integrity through:
  - Users access EMR/EHR through intermediary application and not directly.
  - Authentication
  - Authorisation: separation of duties
  - Auditing
- Clark-Wilson model originally developed for commercial industry.
- This study will be adopting it in context of national EHR system.

References

- Canada Health Infoway. (2006). *EHRS Blueprint: An Interoperable EHR Framework - Version 2*. Retrieved from Canada Health Infoway: https://www.infoway-inforoute.ca/en/component/edocman/resources/technical-documents/391-ehrs-blueprint-v2-full
- CSIR, & Department of Health. (2014). *National Health Normative Standards Framework for Interoperability in eHealth in South Africa - Version 2.0*. Retrieved from SAMED: http://www.samed.org.za/Filemanager/userfiles/hnsf-complete-version.pdf
- Deloitte. (2015). *Independent review of New Zealand's Electronic Health Records Strategy*. Retrieved from Ministry of Health: http://www.health.govt.nz/system/files/documents/publications/independent-review-new-zealand-electronic-health-records-strategy-oct15.pdf
- House of Commons. (2007). *Department of Health: The National Programme for IT in the NHS - Twentieth Report of Session 2006-07*. Retrieved from Parliament: https://publications.parliament.uk/pa/cm200607/cmselect/cmpubacc/390/390.pdf
- Sellberg, N., & Eltes, J. (2017). The Swedish Patient Portal and Its Relation to the National Reference Architecture and the Overall eHealth Infrastructure. In M. Aanestad, M. Grisot, O. Hanseth, & P. Vassilakopoulou (Eds.), *Information Infrastructures within European Health Care* (pp. 225–244). Cham, Switzerland: Springer.

Questions

Thank you