ibime
Informática Biomédica

UNIVERSITAT
POLITÈCNICA
DE VALÈNCIA

Access policies in archetype-based systems

David Moner
damoca@upv.es

Biomedical Informatics Group (IBIME)
ITACA Institute, Technical University of Valencia

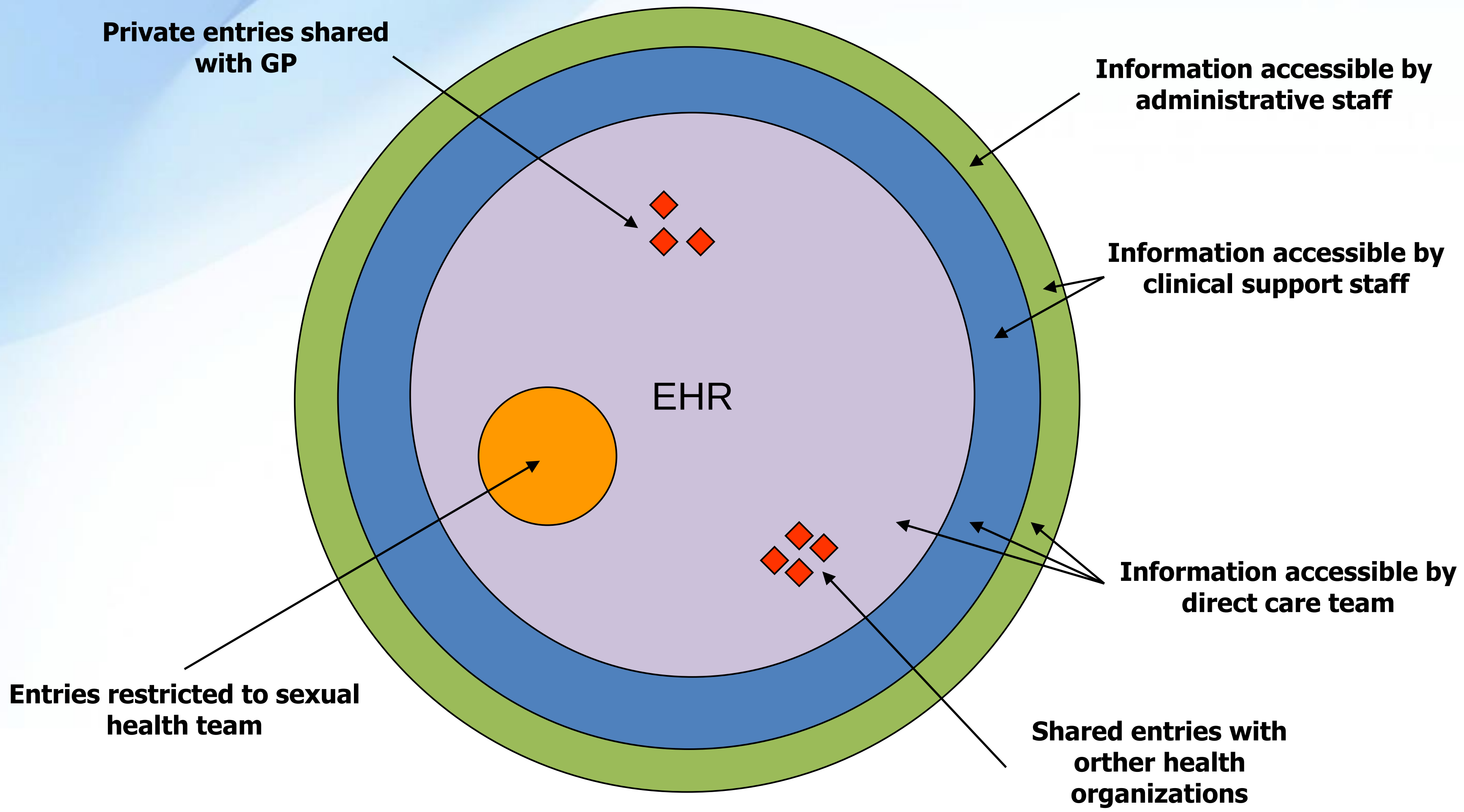
Privacy of health data

- We are the owners of (most of) our clinical data.
  – National and international laws recognize our right to control the access and use of that data.

> Article 5.3. The patient is entitled to object to the disclosure of his or her medical records or information in the records.
>
> *Act of 2 July 1999 No. 63 relating to Patient's Rights (Norway)*

- How could we effectively control who access and uses that information easily?

Privacy of health data



Private entries shared with GP
Information accessible by administrative staff
Information accessible by clinical support staff
EHR
Information accessible by direct care team
Entries restricted to sexual health team
Shared entries with orther health organizations

EN ISO 13606-4 - Security requirements and distribution rules

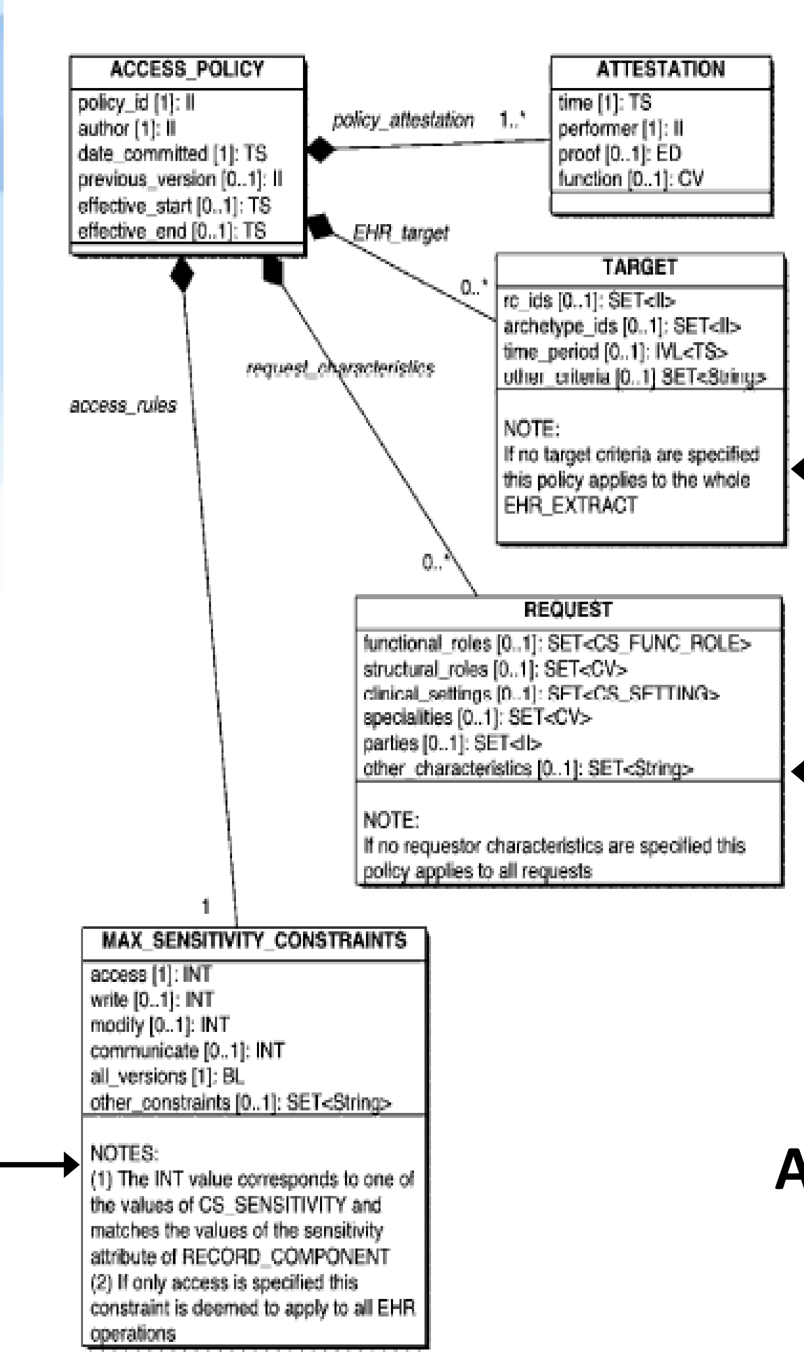
It is a complex problem

AP models	Identity Based Access Control (IBAC), **Role Based Access Control (RBAC)**, Context Based Access Control (CBAC), Attribute Based Access Control (ABAC)…
Technologies	Security Assertion Markup Language (SAML), **eXtensible Access Control Markup Language (XACML)**, eXtensible rights Markup Language (XrML)…
Standards	ISO/TS 22600 (Privilege management and access control), ISO/CD 22857 (Guidelines on data protection to facilitate trans-border flows of personal health information), ISO 27799:2008 (Information security management in health using ISO/IEC 27002)…
Legislation	National Data protection Laws, National Health Data Laws, National Health Research Laws, Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Directive 2001/20/EC on good clinical practice in the conduct of clinical trials on medicinal products for human use…

Archetypes for the definition of access policies

- An Access policy (AP) defines what, who, where, when and how some interaction can be done with an information resource.
- Can we take profit of the archetype approach for the definition of access policies for the EHR?
  - Based on a common reference model.
    - EN ISO 13606 access policy model was designed to communicate access policies, but we can also use it to create new access policies.
  - Facilitates the definition by clinicians and patients.
  - Specialization capabilities.

Access Policy Archetypes (APA)



NOTE:
If no target criteria are specified this policy applies to the whole EHR_EXTRACT

NOTE:
If no requestor characteristics are specified this policy applies to all requests

NOTES:
(1) The INT value corresponds to one of the values of CS_SENSITIVITY and matches the values of the sensitivity attribute of RECORD_COMPONENT
(2) If only access is specified this constraint is deemed to apply to all EHR operations

WHERE it can be done

WHO can do it

WHAT can be done

EN ISO 13606-4 Access Policy model

Archetypes for the definition of access policies

- Who defines those policies?

- We can distinguish three levels of responsibility:
  - Organization/Legislation level
  - Clinical level
  - Personal level

Archetypes for the definition of access policies

- Organizational level
  - Organizations are responsible of enforcing data privacy laws.
  - They also manage information that is not clinical (administrative information).
  - They can create Organizational APAs (O-APA) that define which archetypes are potentially accessible.

Archetypes for the definition of access policies

- Clinical level
  - Health professionals are in charge of deciding which information is clinically relevant or that can be legally hidden to the patient.
  - They create Clinical APAs (C-APA)

> Article 5.1. The patient may be denied access to information in his or her medical records if this is absolutely necessary in order to avoid endangering the patient’s life or serious damage to the patient’s health, or if access is clearly inadvisable out of consideration for persons close to the patient.
>
> *Act of 2 July 1999 No. 63 relating to Patient’s Rights (Norway)*

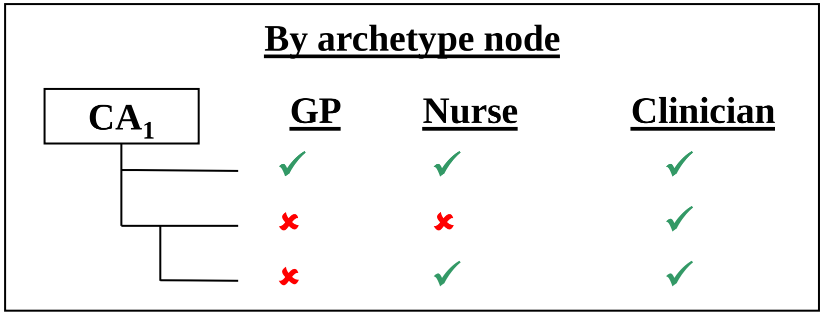
Archetypes for the definition of access policies

- Personal level
  - This is the level that enables patient empowerment of access policies.
  - Any person should be able to define fine-grained rules about who can access to what and under which circumstances.
  - These will be the Personal APA (P-APA).

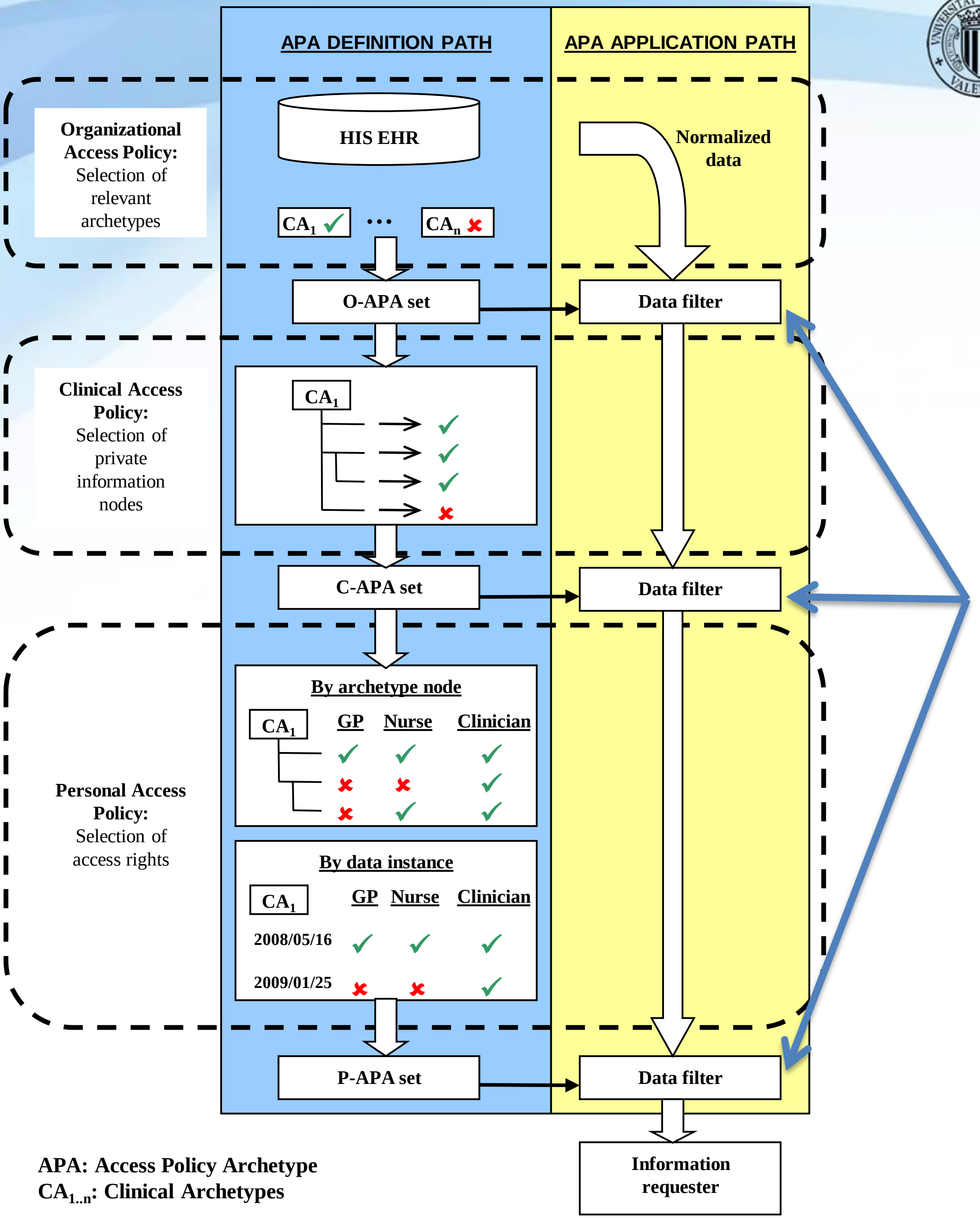
By data instance

CA_1	GP	Nurse	Clinician
2008/05/16	✓	✓	✓
2009/01/25	✗	✗	✓

By archetype node



CA_1	GP	Nurse	Clinician
	✓	✓	✓
	✗	✗	✓
	✗	✓	✓



APA DEFINITION PATH

APA APPLICATION PATH

Organizational Access Policy: Selection of relevant archetypes

Clinical Access Policy: Selection of private information nodes

Personal Access Policy: Selection of access rights

By archetype node

CA_1	GP	Nurse	Clinician
	✓	✓	✓
	✗	✗	✓
	✗	✓	✓

By data instance

CA_1	GP	Nurse	Clinician
2008/05/16	✓	✓	✓
2009/01/25	✗	✗	✓

SELECT …
FROM …
WHERE …

APA: Access Policy Archetype
$CA_{1..n}$: Clinical Archetypes

Challenges

- Definition
  - All the EHR must be archetyped.
  - Shared ontology for professional roles.
  - Shared infrastructure for professional identifiers.
- Execution
  - Convert APAs into XACML or other industry-standard compliant AP.
  - Ensure that the filtered results are still clinically and technically valid.

Thank you for your attention!

Questions?

This presentation has been supported by a grant from Iceland, Liechtenstein and Norway through the EEA Financial Mechanism. Operated by Universidad Complutense de Madrid

NILS mobility project

ICELAND
LIECHTENSTEIN
NORWAY
eea grants