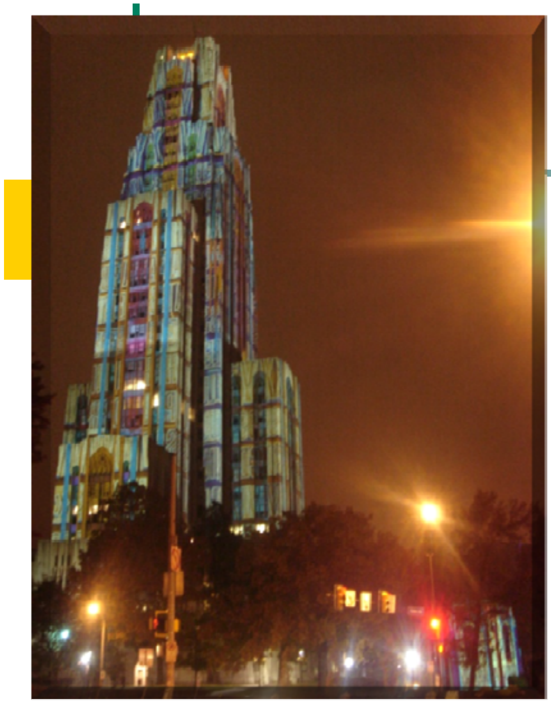
IS 2150 / TEL 2810
Introduction to Security



James Joshi
Professor, SIS

Nov 22, 2016

Healthcare IT Security

Clinical Information Systems Security Policy

(Bishop’s Book)

Clinical Information Systems Security Policy

- Intended for medical records
  - Conflict of interest not critical problem
  - Patient confidentiality, authentication of records and annotators, and integrity are
- Entities:
  - Patient: subject of medical records (or agent on his behalf)
  - Personal health information: data about patient's health or treatment enabling identification of patient
  - Clinician: health-care professional with access to personal health information while doing job

Assumptions and Principles

- Assumes health information involves 1 person at a time
  - Not always true; OB/GYN involves father as well as mother
- Principles derived from medical ethics of various societies, and from practicing clinicians
  - Similar to the certification and enforcement rules

Access

- Principle 1:

  Each medical record has an access control list naming the individuals or groups who may read and append information to the record. The system must restrict access to those identified on the access control list.

  - Idea is that:
    - Clinicians need access, but no-one else.
    - Auditors get access to copies, so they cannot alter records
- Principle 2:

  One of the clinicians on the access control list must have the right to add other clinicians to the access control list.

  - Called the *responsible clinician*

Access

- Principle 3:

  The responsible clinician must notify the patient of the names on the access control list whenever the patient’s medical record is opened. Except for situations given in statutes, or in cases of emergency, the responsible clinician must obtain the patient’s consent.

  - Patient must consent to all treatment, and must know of accesses / violations of security

Access

- Principle 4:

  The name of the clinician, the date, and the time of the access of a medical record must be recorded. Similar information must be kept for deletions.

  - This is for auditing.
    - Don’t delete information;
    - Update it (last part is for deletion of records after death, for example, or deletion of information when required by statute).
    - Record information about all accesses.

Record Creation & Info Deletion

- Creation Principle:

  A clinician may open a record, with the clinician and the patient on the access control list. If a record is opened as a result of a referral, the referring clinician may also be on the access control list.

  - Creating clinician needs access, and patient should get it.
  - If created from a referral, referring clinician needs access to get results of referral.

Deletion & Confinement

- Deletion Principle:

  Clinical information cannot be deleted from a medical record until the appropriate time has passed.

  - This varies with circumstances.
- Confinement Principle:

  Information from one medical record may be appended to a different medical record if and only if the access control list of the second record is a subset of the access control list of the first.

  - This keeps information from leaking to unauthorized users.
  - All users have to be on the access control list.

Aggregation

- Principle:

  Measures for preventing aggregation of patient data must be effective. In particular, a patient must be notified if anyone is to be added to the access control list for the patient's record and if that person has access to a large number of medical records.

  - Fear here is that a corrupt investigator may obtain access to a large number of records, correlate them, and discover private information about individuals which can then be used for nefarious purposes (such as blackmail)

Enforcement

- Principle:

  Any computer system that handles medical records must have a subsystem that enforces the preceding principles. The effectiveness of this enforcement must be subject to evaluation by independent auditors.

  - This policy has to be enforced, and the enforcement mechanisms must be auditable (and audited)

Compared to Bell-LaPadula

- Confinement Principle imposes lattice structure on entities in model
  - Similar to Bell-LaPadula
- CISS focuses on objects being accessed; B-LP on the subjects accessing the objects
  - May matter when looking for insiders

Compared to Clark-Wilson

- CDIs are medical records and associated ACLs
- TPs are functions updating records, ACLs
- IVPs certify:
    - A person identified as a clinician is a clinician;
    - A clinician validates, or has validated, information in the medical record;
    - When someone is to be notified of an event, such notification occurs; and
    - When someone must give consent, the operation cannot proceed until the consent is obtained
- Auditing (CR4) requirement: make all records append-only, notify patient when access control list changed

Anytime, anywhere access to secure, Privacy-aware Healthcare Services: Issues, Approaches & Challenges

Mohd. Anwar, James Joshi, Joseph Tan

(Health Policy and Technology Journal)

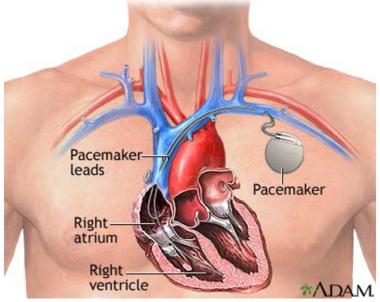
Anywhere, Anytime Healthcare *Secure and privacy-aware*

- Enablers of this new paradigm
  - E-health informatics
  - Sensor technologies
  - Mobile devices (including smart phones)
- Value added features
  - Monitoring devices and On-time intervention
  - Integrated Care
  - Self-care
  - Social Support

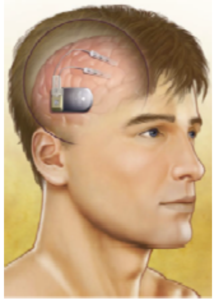
Monitoring devices and On-time intervention

- Miniaturization of sensor devices + wireless
  - “Remote monitoring cuts patient dealth by 45%” (Dept of Health, UK Report) – help intervene
    - Blood pressure, sugar, etc.
- Monitoring beneficial for atleast
  - Lifestyle and general well being monitoring
  - Chronic disease or condition management
    - Cardian arrhythmia, diabetes, ..
  - Clinical workflow mgmt
    - Telehealth, face-to-face care, in-patient care workflow, ..

Monitoring devices and On-time intervention



- Health status monitoring device types;
  - In-body: implantable devices
    - Pacemakers, defibrillators, neurostimulators (physiological conditions)
    - Wireless; implant reader receives data
  - On-body: wearable
    - Motion sensors, blood pressure meters
  - Additional monitory of environment is also important
    - Katz's ADL (Activities for Daily Living: bathing, dressing, toileting,..) – for Geriatic care (elderly patients)

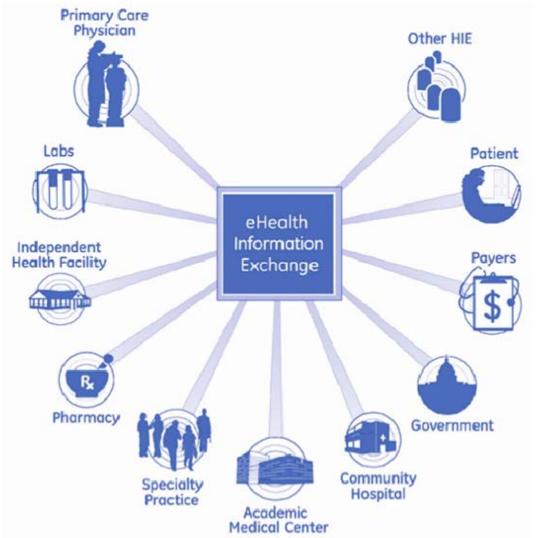


- RFID (Radio Frequency Identification)
  - Can be used for monitoring medical assets –
    - e.g., attach an RFID tag to an implantable device;
    - Use it to for device identification RFID reader can be in smart phone

Integrated Care

- Typical patient treatment may involve
  - Physician → diagnostic lab → prescription
  - Physician need info generated by other care givers
    - Health records have info from several care givers; may relate to multiple diseases, …
    - Maybe fragmented; dispersed across providers
    - COORDINATION is critical
  - Mobile lifestyle – services should be available
    - Integration needed :
      - Across the hospitals; cross-border, etc.
    - Nationwide health Information Network (NHIN)
      - Information sharing among federal agencies, hospitals, and doctors' offices

Integrated Care



- Integration is key
  - Consolidate healthcare services and workflow: horizontal & vertical integratior
  - Horizontal –
    - Among independent healthcare provides
    - e.g., integrate hospitals and nursing homes
  - Vertical –
    - Combine/coordinate interdependent service providers
    - e.g., integrate primary care and specialty care

Self-Care

- Self-care behaviors
    - Seeking relevant health information and evaluation of options
    - Monitoring ones vital signs
    - Maintaining healthy lifestyle choices
    - Making informed decisions about one’s health
    - Center piece of self management is: *Personal Health Record* (PHR) [may include Gene info in future]
  - Decision support tools need to be integrated with PHR
  - Current PHR systems
    - Microsoft’s Health Vault; The Patient Portal, MyChart, MyOscar
    - About 70M in US have access to PHR systems
  - New Frontiers: SmartPhone Apps
    - BMI cal; RunKeeper, CDC Vaccine Schedule, SleepBot, etc.

Social Support

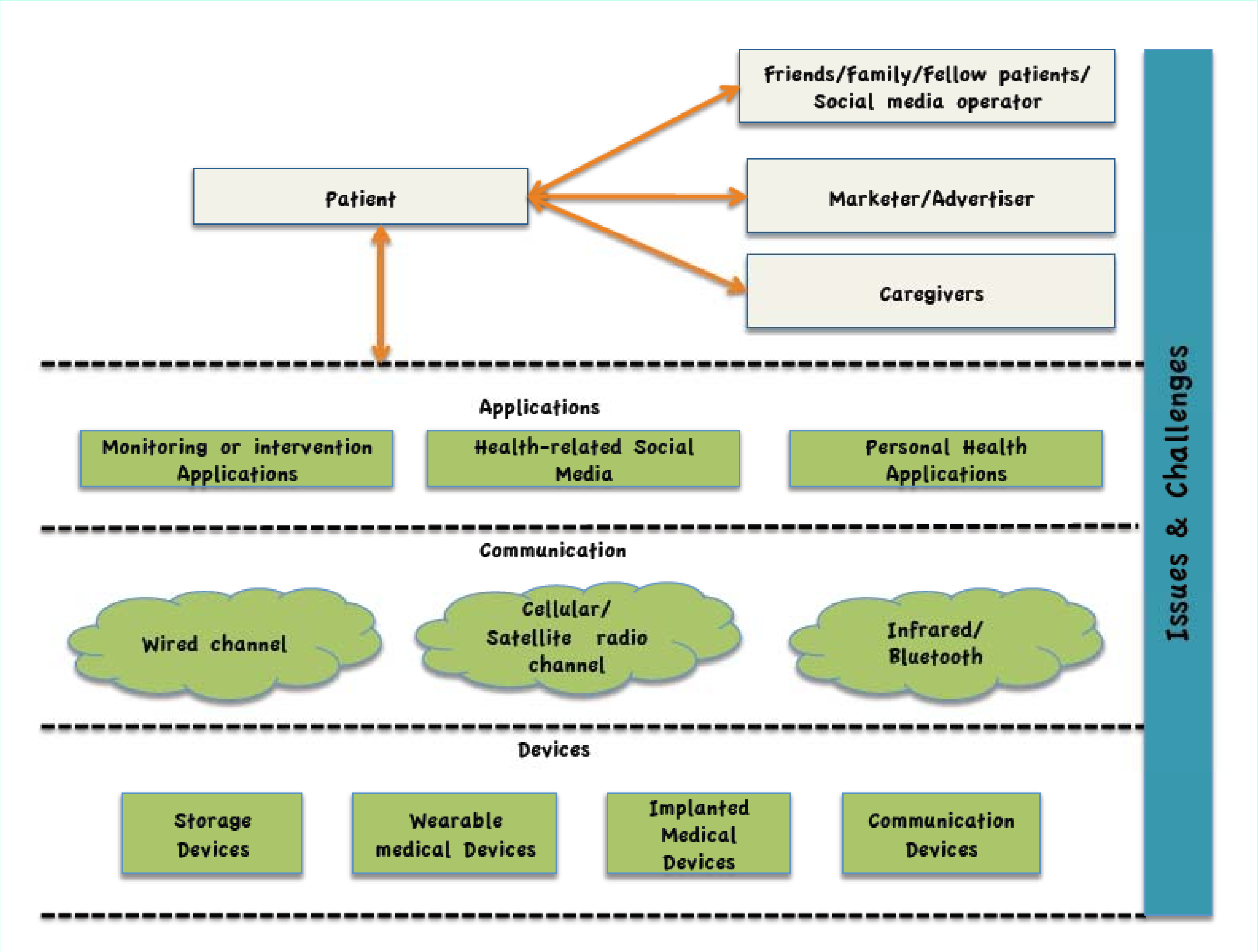
- Social connectedness/support
  - Provides mechanisms to help in health & wellbeing
    - Collective sharing (patientslikeme.org)
    - BodySpace – social fitness and weight-loss app
    - Need to be careful about misinformation !
  - Healthcare social network is on the rise
    - Relevant research at LERSAIS:

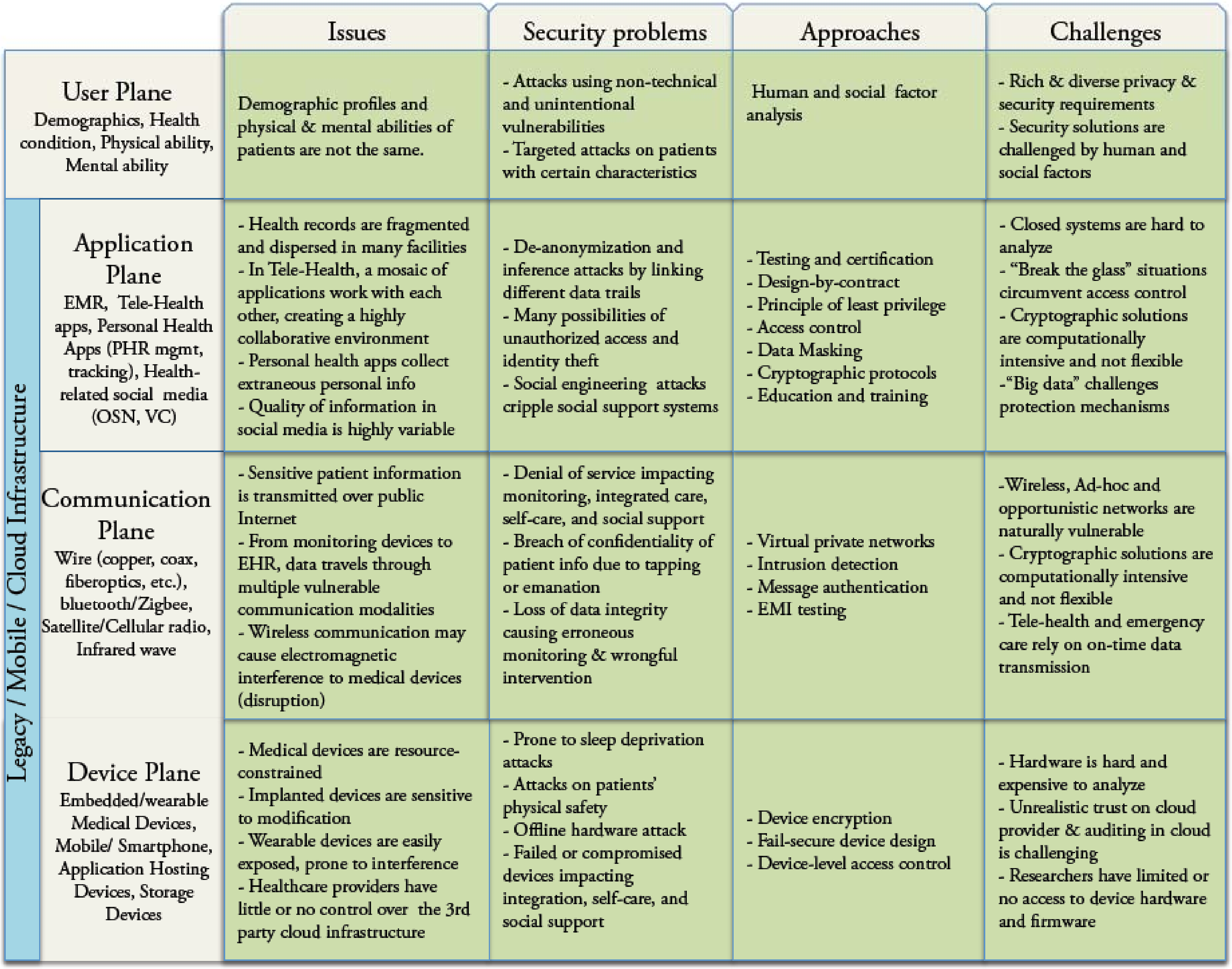
      LEAF for IPV survivors (Intimate Partner Violence)
      - Community of: Care providers, friends/family, legal and social entities, mentors (survivors)
      - Privacy is key

      (Talk to Prof. Palanisamy and Me)

YouTube: https://www.youtube.com/watch?v=YfsRJWgwncU&feature=youtu.be

Security and Privacy Issues/Challenges


Friends/family/fellow patients/ Social media operator
Patient
Marketer/Advertiser
Caregivers
Applications
Monitoring or intervention Applications
Health-related Social Media
Personal Health Applications
Communication
Wired channel
Cellular/ Satellite radio channel
Infrared/ Bluetooth
Devices
Storage Devices
Wearable medical Devices
Implanted Medical Devices
Communication Devices
Issues & Challenges



		Issues	Security problems	Approaches	Challenges
	User Plane Demographics, Health condition, Physical ability, Mental ability	Demographic profiles and physical & mental abilities of patients are not the same.	- Attacks using non-technical and unintentional vulnerabilities - Targeted attacks on patients with certain characteristics	Human and social factor analysis	- Rich & diverse privacy & security requirements - Security solutions are challenged by human and social factors
Legacy / Mobile / Cloud Infrastructure	Application Plane EMR, Tele-Health apps, Personal Health Apps (PHR mgmt, tracking), Health-related social media (OSN, VC)	- Health records are fragmented and dispersed in many facilities - In Tele-Health, a mosaic of applications work with each other, creating a highly collaborative environment - Personal health apps collect extraneous personal info - Quality of information in social media is highly variable	- De-anonymization and inference attacks by linking different data trails - Many possibilities of unauthorized access and identity theft - Social engineering attacks cripple social support systems	- Testing and certification - Design-by-contract - Principle of least privilege - Access control - Data Masking - Cryptographic protocols - Education and training	- Closed systems are hard to analyze - "Break the glass" situations circumvent access control - Cryptographic solutions are computationally intensive and not flexible -"Big data" challenges protection mechanisms
	Communication Plane Wire (copper, coax, fiberoptics, etc.), bluetooth/Zigbee, Satellite/Cellular radio, Infrared wave	- Sensitive patient information is transmitted over public Internet - From monitoring devices to EHR, data travels through multiple vulnerable communication modalities - Wireless communication may cause electromagnetic interference to medical devices (disruption)	- Denial of service impacting monitoring, integrated care, self-care, and social support - Breach of confidentiality of patient info due to tapping or emanation - Loss of data integrity causing erroneous monitoring & wrongful intervention	- Virtual private networks - Intrusion detection - Message authentication - EMI testing	-Wireless, Ad-hoc and opportunistic networks are naturally vulnerable - Cryptographic solutions are computationally intensive and not flexible - Tele-health and emergency care rely on on-time data transmission
	Device Plane Embedded/wearable Medical Devices, Mobile/ Smartphone, Application Hosting Devices, Storage Devices	- Medical devices are resource-constrained - Implanted devices are sensitive to modification - Wearable devices are easily exposed, prone to interference - Healthcare providers have little or no control over the 3rd party cloud infrastructure	- Prone to sleep deprivation attacks - Attacks on patients' physical safety - Offline hardware attack - Failed or compromised devices impacting integration, self-care, and social support	- Device encryption - Fail-secure device design - Device-level access control	- Hardware is hard and expensive to analyze - Unrealistic trust on cloud provider & auditing in cloud is challenging - Researchers have limited or no access to device hardware and firmware

Epilepsy attacks
Phishing

Capture device id, location, demographic

Summary

- CISS policy derived from medical ethics and practices

- Security HealthCare IT Environment
  - S&P Issues from various domains/levels
  - IoT – medical devices – adds to safety issues
  - HealthCloud
  - Health SN
    - Cyber Physical Social systems environment

Patient-centric Authorization Framework for Sharing Electronic Health Records

Jing Jin et al.

(ACM SACMAT)

Outline

Part I – Overview

Part II – Patient-centric authorization model

Part III – EHR sharing system

Part IV – Conclusion

What is EHR?

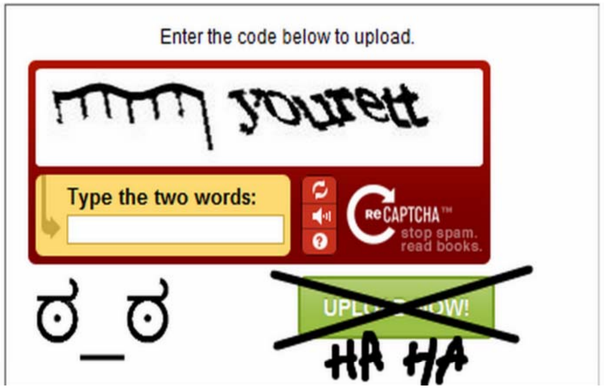
IOM(Institute of Medicine) (1991)
"……an electronic patient record that resides in a system specifically designed to support users through availability of complete and accurate data, practitioner reminders and alerts, clinical decision support systems, links to bodies of medical knowledge and other aids."

Illustration by Chris Twichell

Why EHR?

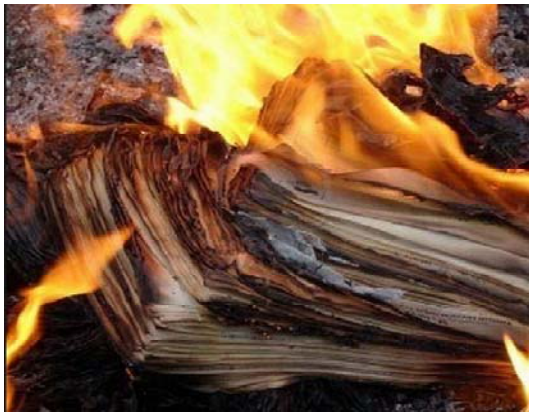
Paperless.

Readable.



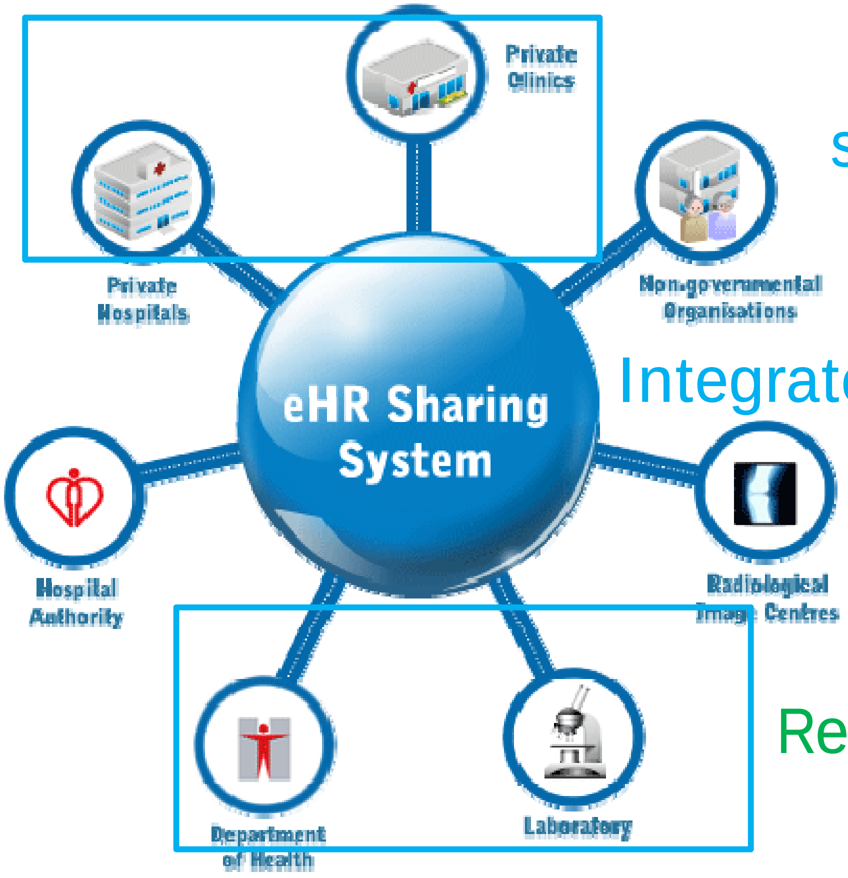
Enter the code below to upload.

Safe(?).



Access anywhere.

Sharing Electronic Health Records



Treatment

scattered

Integrated, unified

Research,Study

Patient-centric Authorization

Not user, but owner controls the access to data!

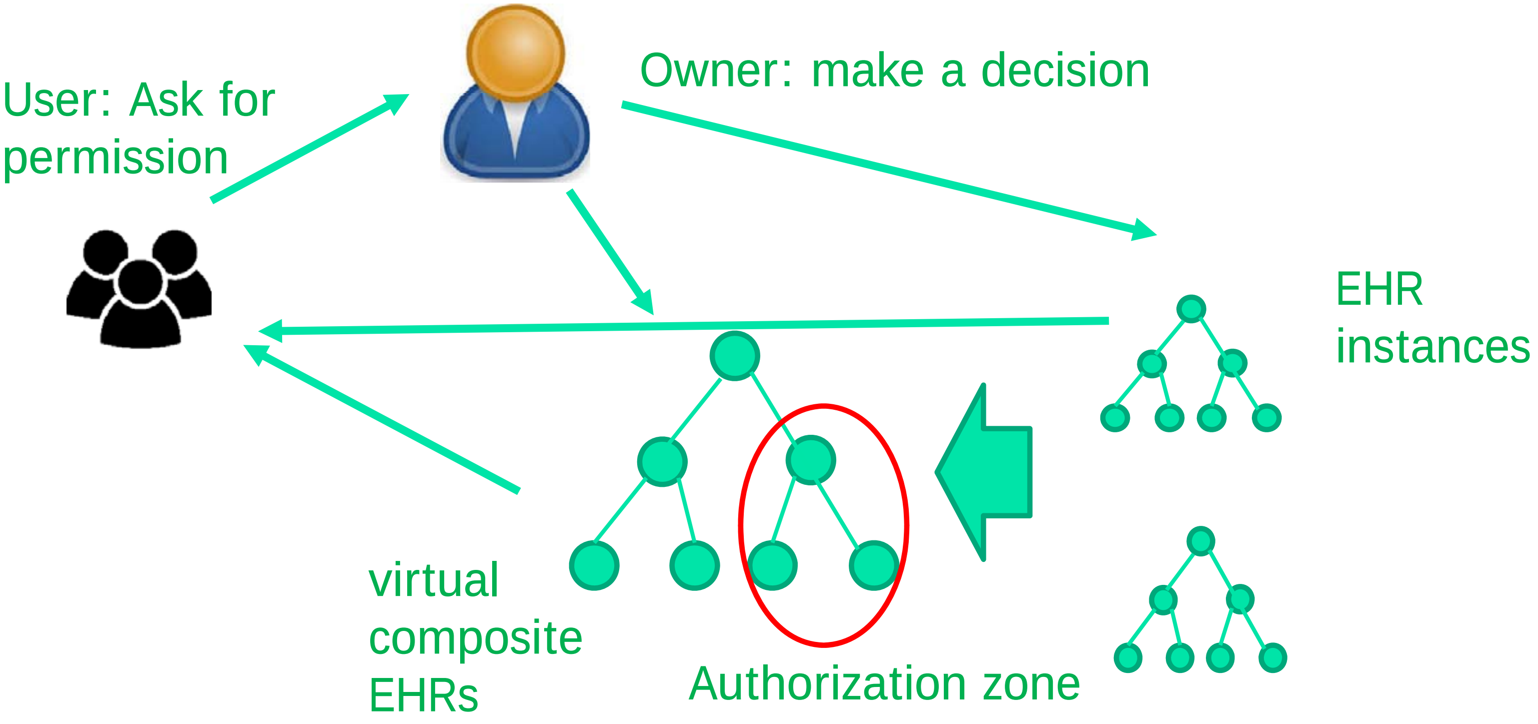
Why owner?

1. The sensitivity of data is different for different patients
2. The role (relationship) of user is dynamic
3. Need to know (access purpose)

To support this, the patient should ultimately own his or her medical records and be responsible for maintaining access rights for the distributed EHRs.

Contribution of this paper:

1. A model with hierarchical structure and a unified policy scheme for uniformly regulating selective sharing of both discrete EHR instances and the aggregated virtual composite EHRs at different levels of granularity.



Contribution of this paper:

2. Mechanisms that identify and resolve potential policy anomalies for composed access control policies at the virtual composite EHR level.

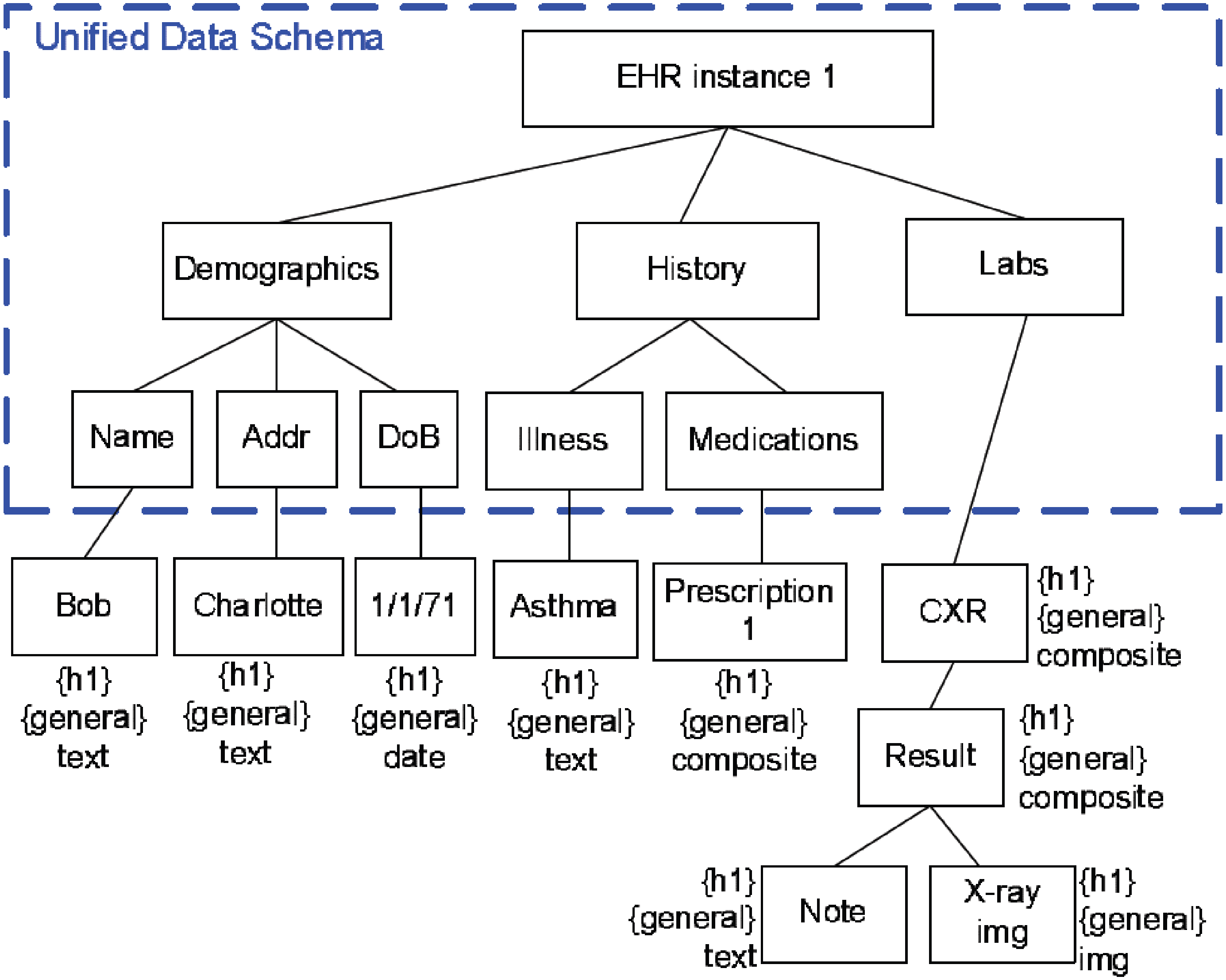
3. Implementation and evaluation.
a virtual composite EHR sharing system is designed and implemented.

Patient-centric authorization model

Unified Logical EHR Model
A. Understand the model

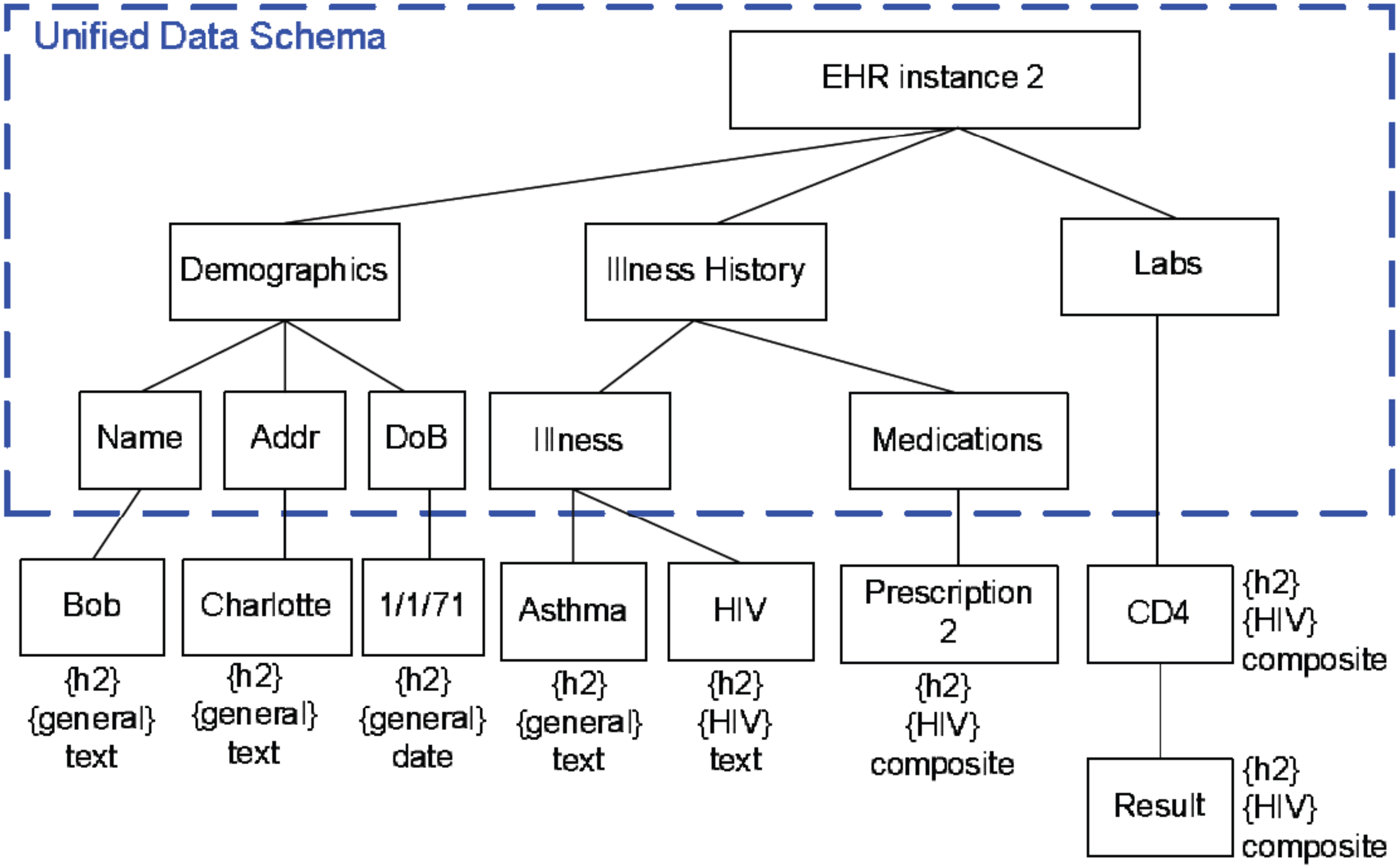
1. Unified Data Schema (UDS).（assumption）
2. Nodes.
3. Edges.
4. Properties. <origin, sensitivity, object type>

Patient-centric authorization model



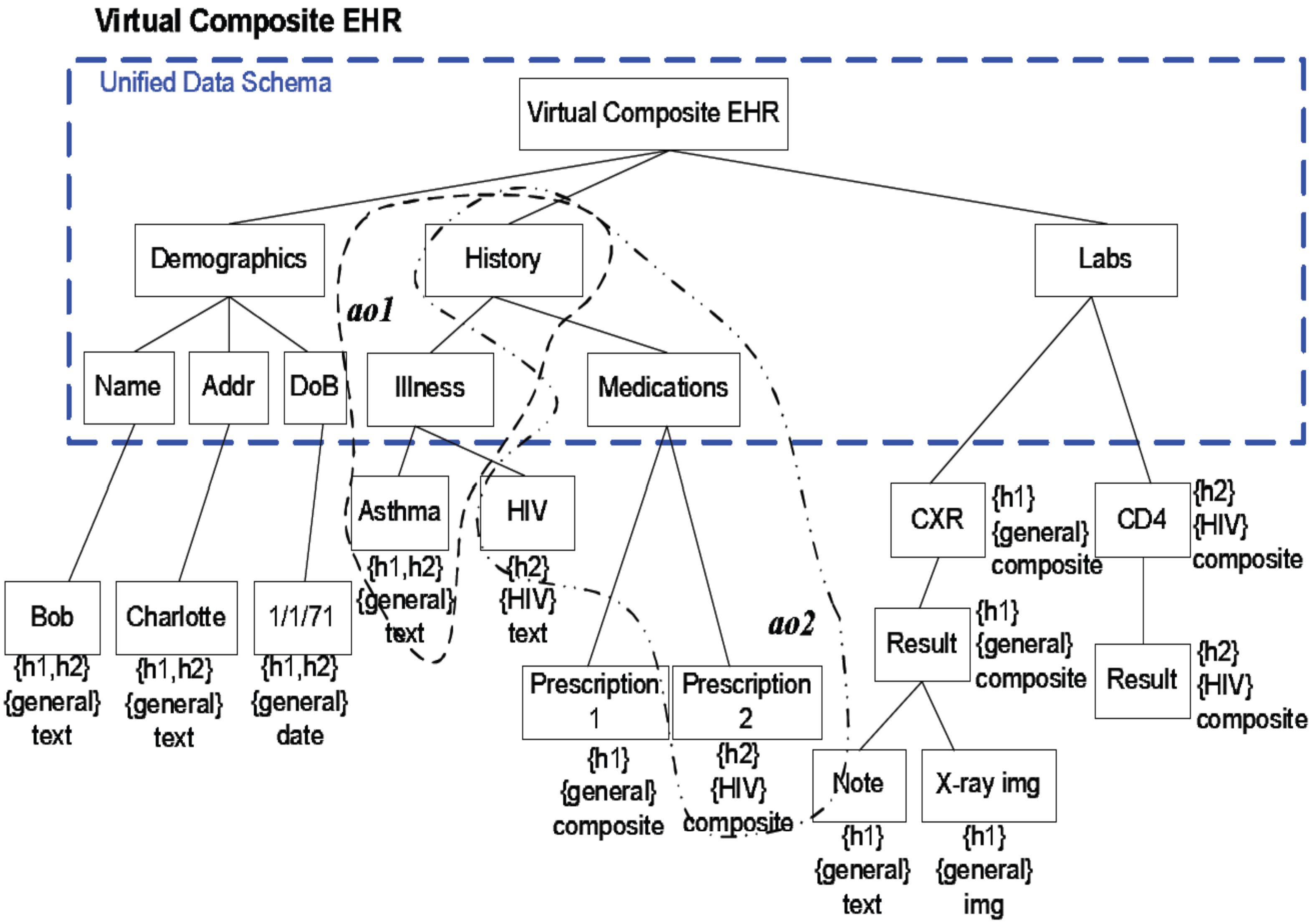
a. EHR instance 1 (Hospital 1)

Patient-centric authorization model



b. EHR instance 2 (Hospital 2)

Patient-centric authorization model



Patient-centric authorization model

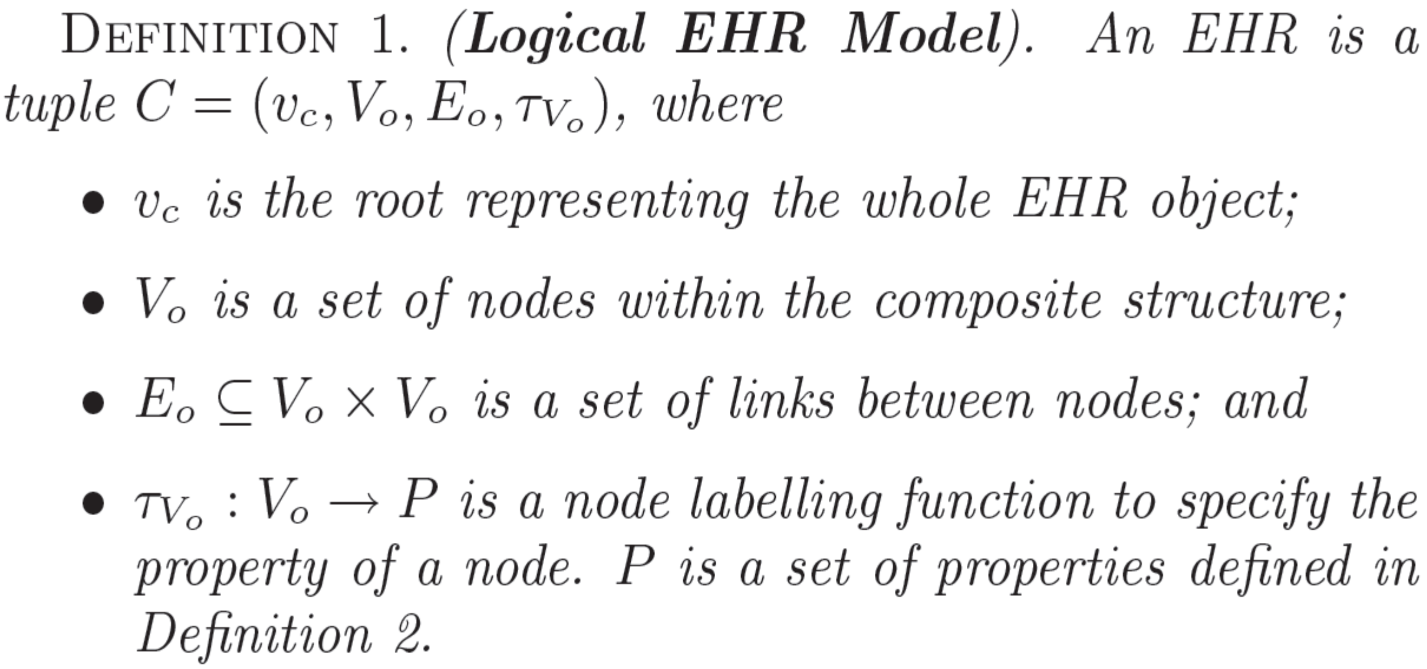
B. Expression of the model – policy specification

8 definitions...and 3 examples.

1. Logical EHR Model.
2. Property.
3. Subject Specification.
4. Filtration Property.
5. Property Match.
6. Object Specification.
7. Intended Purpose.
8. Access Control Policy.

Patient-centric authorization model

1. Logical EHR Model.

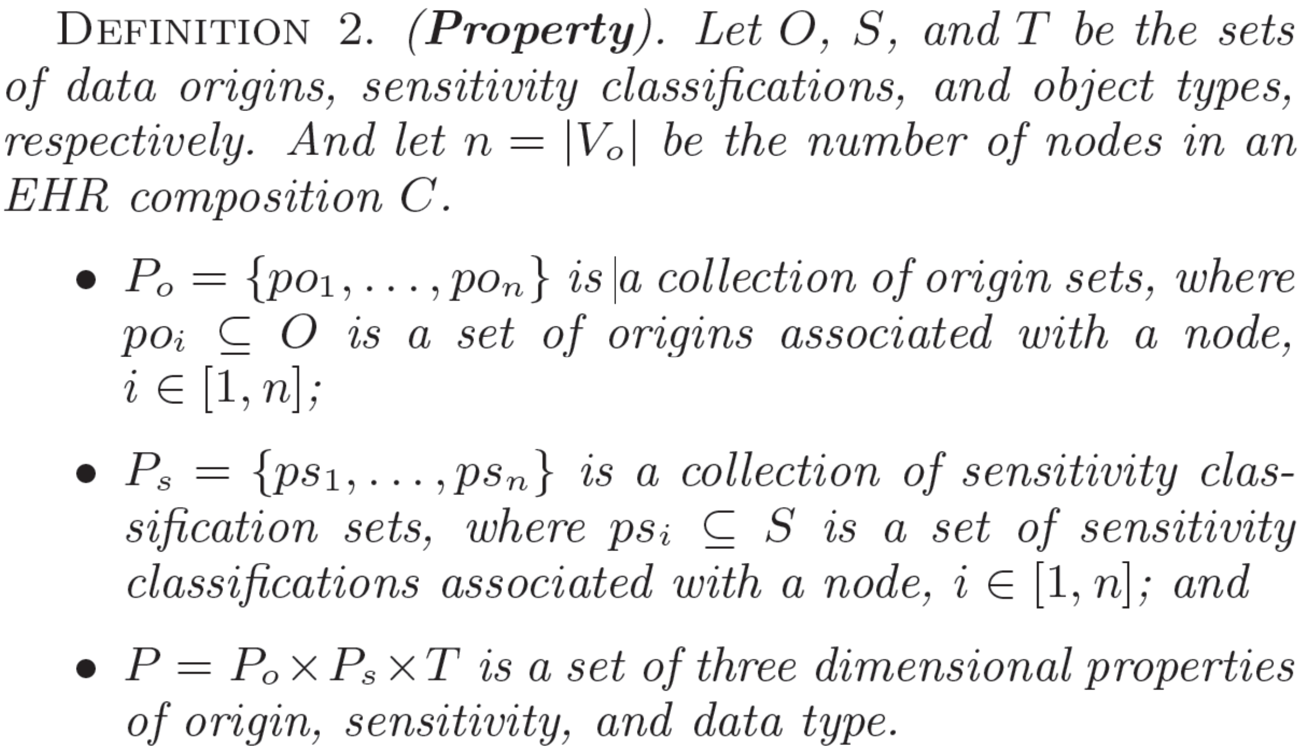


Definition 1. *(**Logical EHR Model**). An EHR is a tuple* $C = (v_c, V_o, E_o, \tau_{V_o})$*, where*

- v_c *is the root representing the whole EHR object;*
- V_o *is a set of nodes within the composite structure;*
- $E_o \subseteq V_o \times V_o$ *is a set of links between nodes; and*
- $\tau_{V_o} : V_o \rightarrow P$ *is a node labelling function to specify the property of a node.* P *is a set of properties defined in Definition 2.*

Patient-centric authorization model

2. Property.



DEFINITION 2. (***Property***). *Let O, S, and T be the sets of data origins, sensitivity classifications, and object types, respectively. And let $n = |V_o|$ be the number of nodes in an EHR composition C.*

- $P_o = \{po_1, \ldots, po_n\}$ *is a collection of origin sets, where* $po_i \subseteq O$ *is a set of origins associated with a node,* $i \in [1, n]$*;*
- $P_s = \{ps_1, \ldots, ps_n\}$ *is a collection of sensitivity classification sets, where* $ps_i \subseteq S$ *is a set of sensitivity classifications associated with a node,* $i \in [1, n]$*; and*
- $P = P_o \times P_s \times T$ *is a set of three dimensional properties of origin, sensitivity, and data type.*

Patient-centric authorization model

Path expression

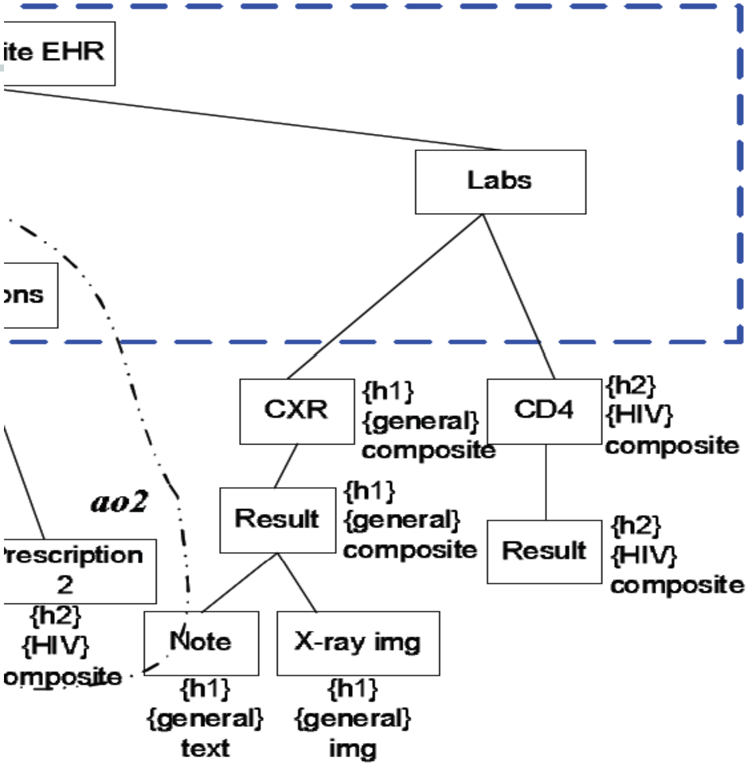
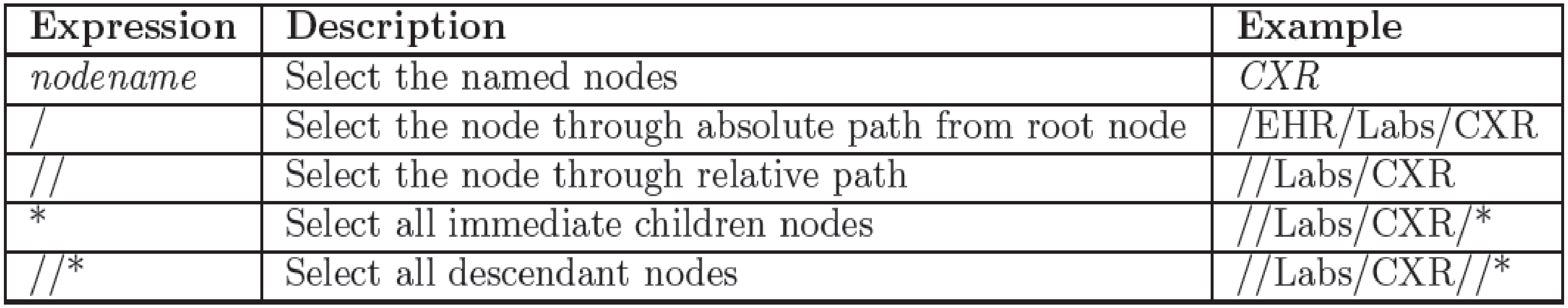


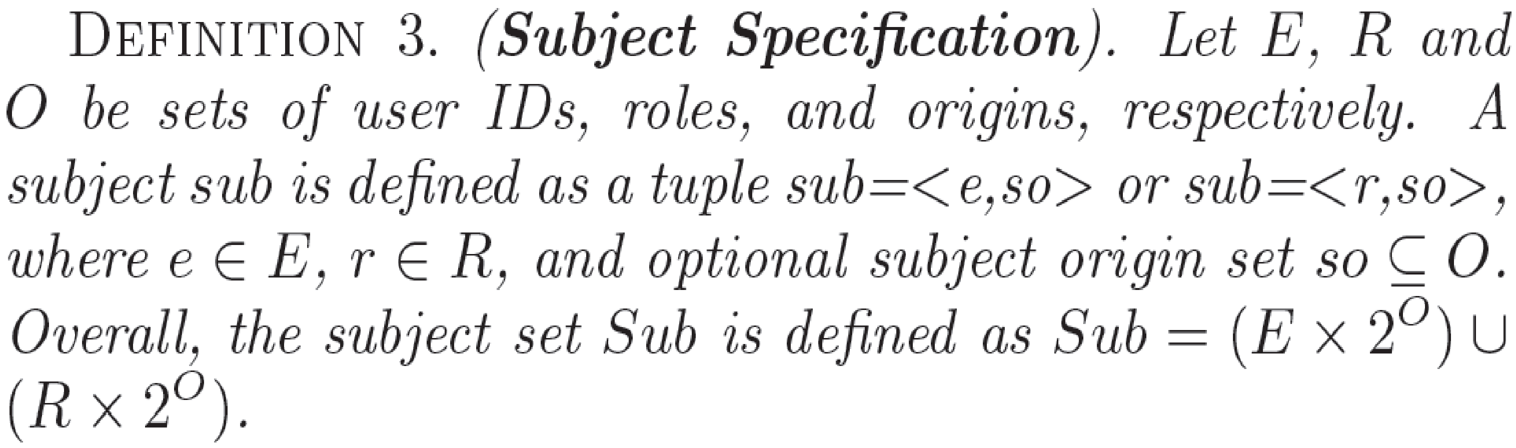
Table 1: Path Expression for Node Selection



Expression	Description	Example
nodename	Select the named nodes	*CXR*
/	Select the node through absolute path from root node	/EHR/Labs/CXR
//	Select the node through relative path	//Labs/CXR
*	Select all immediate children nodes	//Labs/CXR/*
//*	Select all descendant nodes	//Labs/CXR//*

Patient-centric authorization model

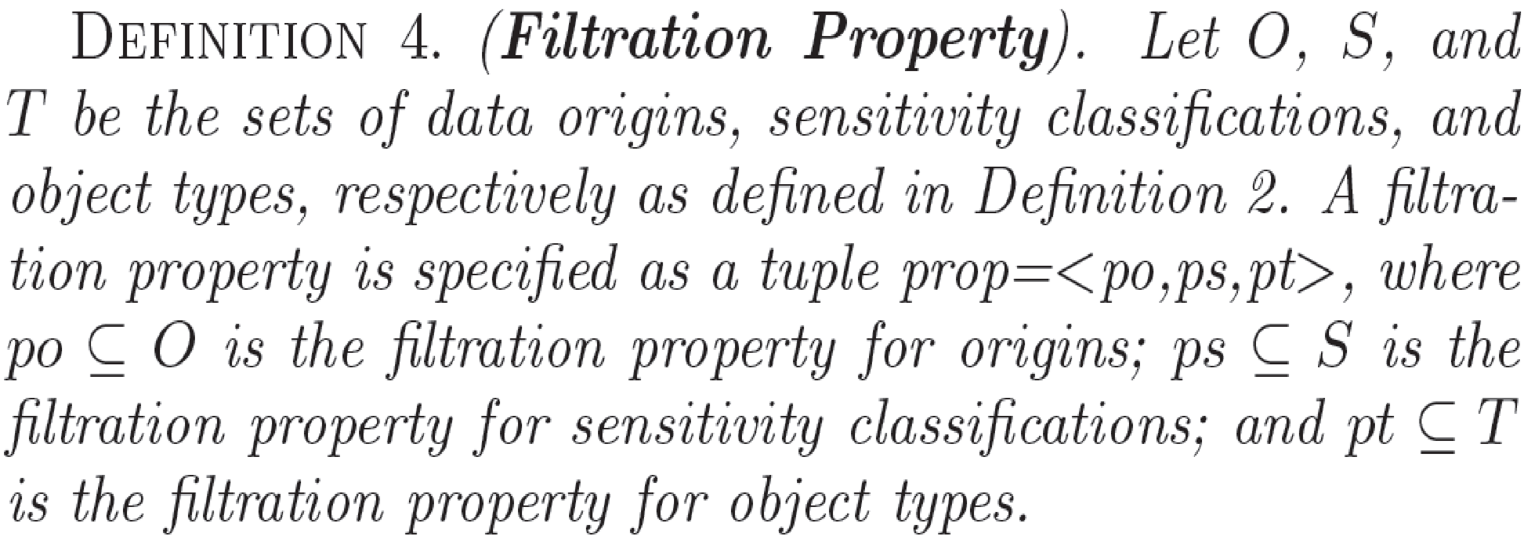
3. Subject Specification.



DEFINITION 3. ***(Subject Specification).*** *Let E, R and O be sets of user IDs, roles, and origins, respectively. A subject sub is defined as a tuple sub=<e,so> or sub=<r,so>, where $e \in E$, $r \in R$, and optional subject origin set so $\subseteq O$. Overall, the subject set Sub is defined as $Sub = (E \times 2^O) \cup (R \times 2^O)$.*

Patient-centric authorization model

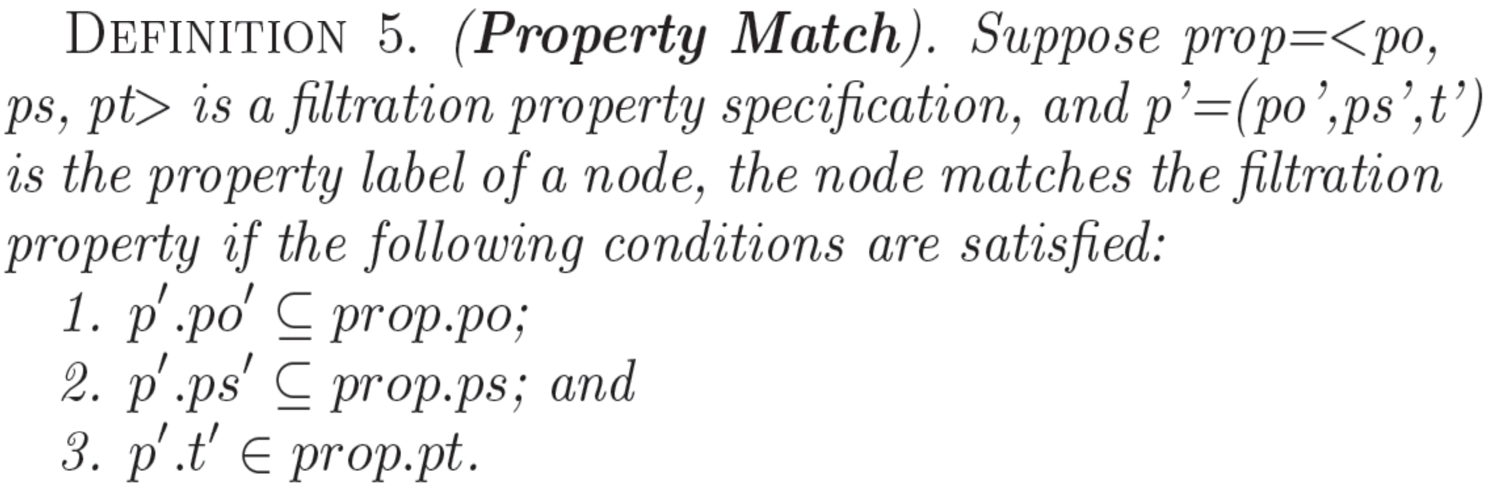
4. Filtration Property.



DEFINITION 4. (***Filtration Property***). *Let O, S, and T be the sets of data origins, sensitivity classifications, and object types, respectively as defined in Definition 2. A filtration property is specified as a tuple prop=<po,ps,pt>, where po $\subseteq O$ is the filtration property for origins; ps $\subseteq S$ is the filtration property for sensitivity classifications; and pt $\subseteq T$ is the filtration property for object types.*

Patient-centric authorization model

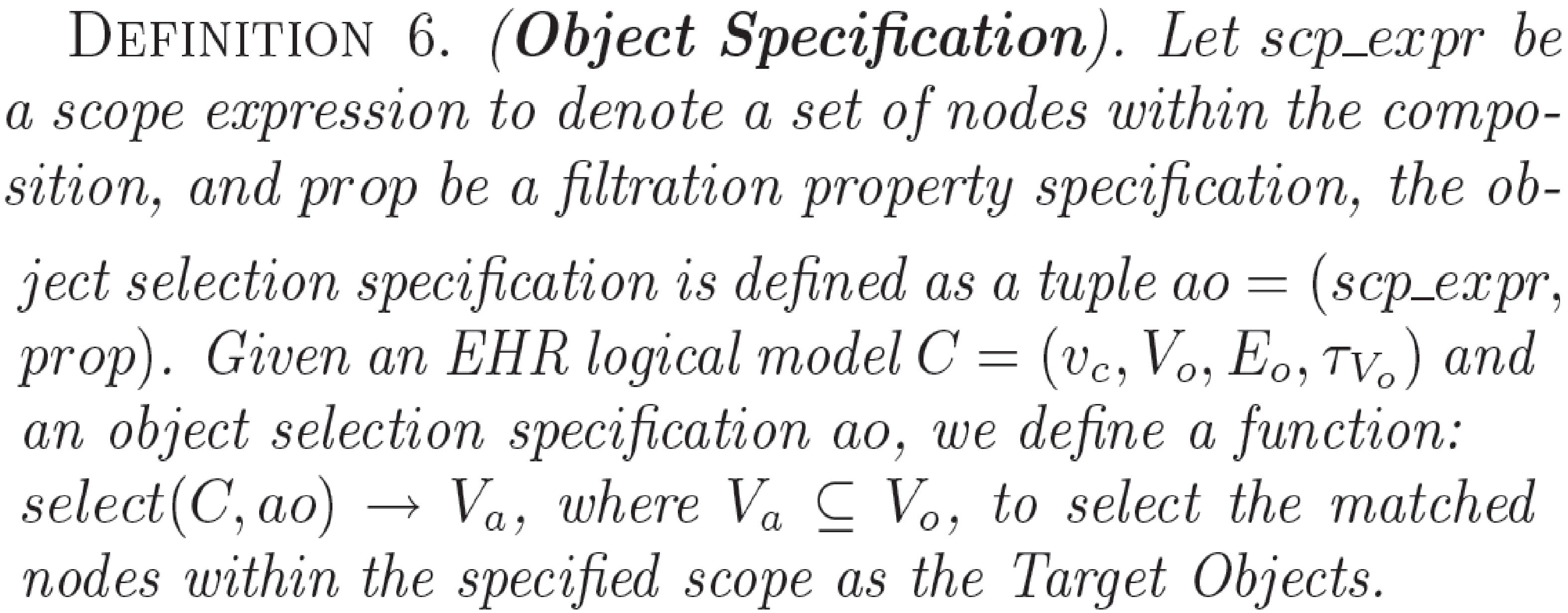
5. Property Match.



DEFINITION 5. (***Property Match***). *Suppose prop=<po, ps, pt> is a filtration property specification, and p'=(po',ps',t') is the property label of a node, the node matches the filtration property if the following conditions are satisfied:*

1. $p'.po' \subseteq prop.po$;
2. $p'.ps' \subseteq prop.ps$; *and*
3. $p'.t' \in prop.pt$.

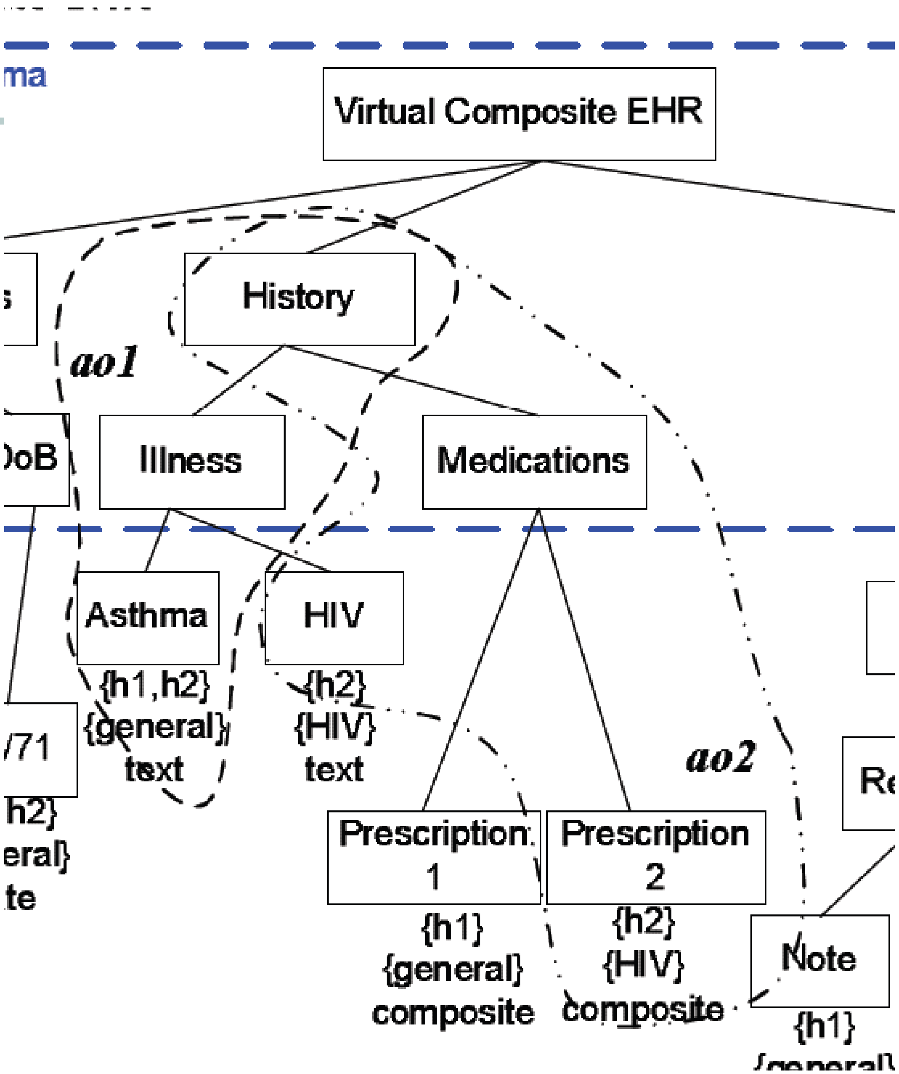
6. Object Specification.



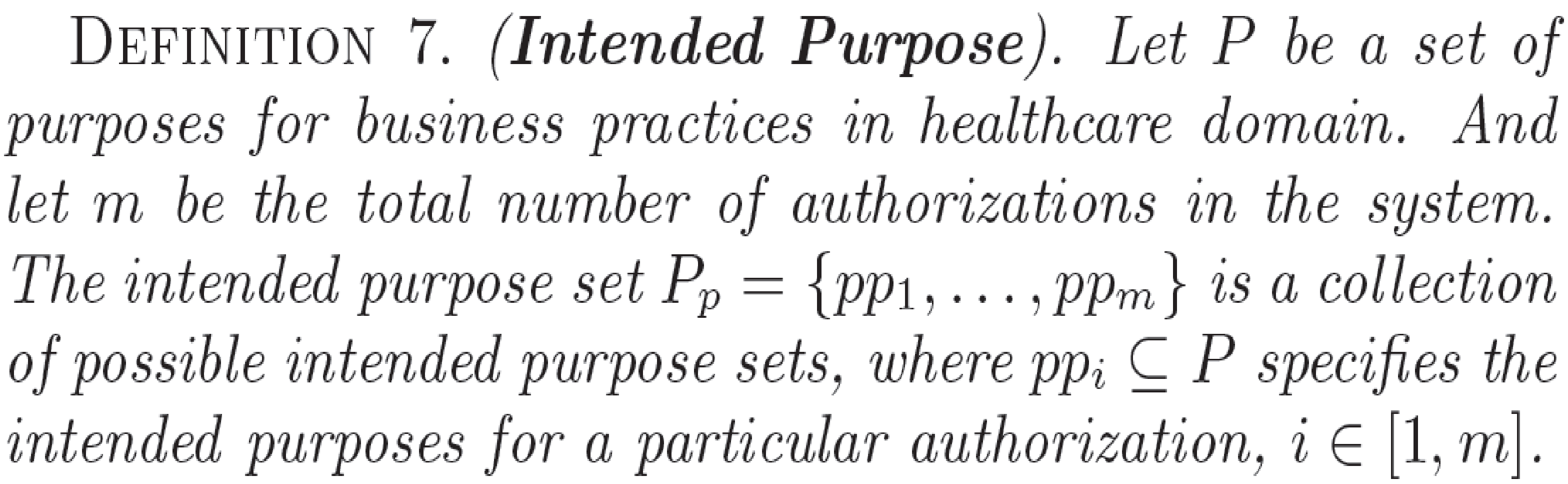
DEFINITION 6. *(**Object Specification**). Let scp_expr be a scope expression to denote a set of nodes within the composition, and prop be a filtration property specification, the object selection specification is defined as a tuple $ao = (scp\_expr, prop)$. Given an EHR logical model $C = (v_c, V_o, E_o, \tau_{V_o})$ and an object selection specification ao, we define a function: $select(C, ao) \rightarrow V_a$, where $V_a \subseteq V_o$, to select the matched nodes within the specified scope as the Target Objects.*

ao1:
ao1=(/VirtualEHR/History//*,<{h2},{general},*>);

ao2:
ao2=(/VirtualEHR/History//*,<{*},{HIV},*>).

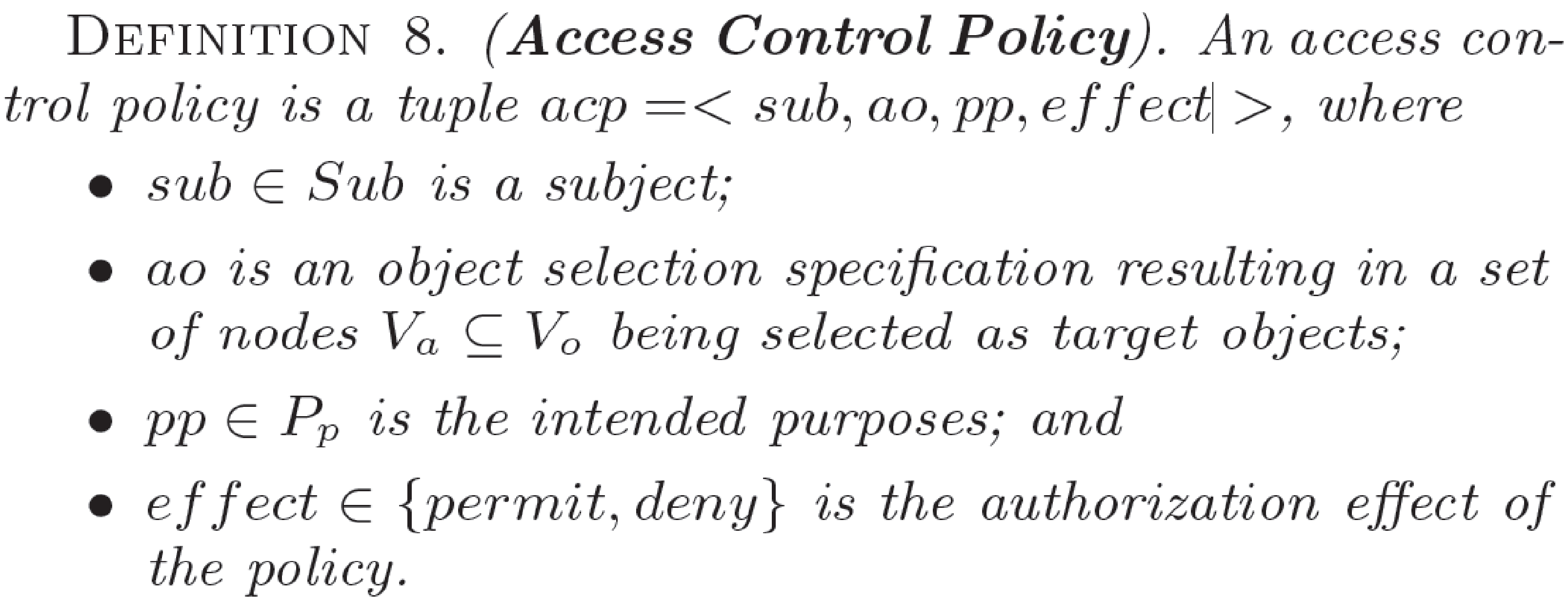


7. Intended Purpose.



DEFINITION 7. (***Intended Purpose***). *Let P be a set of purposes for business practices in healthcare domain. And let m be the total number of authorizations in the system. The intended purpose set $P_p = \{pp_1, \ldots, pp_m\}$ is a collection of possible intended purpose sets, where $pp_i \subseteq P$ specifies the intended purposes for a particular authorization, $i \in [1, m]$.*

8. Access Control Policy.



DEFINITION 8. (***Access Control Policy***). *An access control policy is a tuple* $acp =< sub, ao, pp, effect| >$, *where*

- $sub \in Sub$ *is a subject;*
- *ao is an object selection specification resulting in a set of nodes* $V_a \subseteq V_o$ *being selected as target objects;*
- $pp \in P_p$ *is the intended purposes; and*
- $effect \in \{permit, deny\}$ *is the authorization effect of the policy.*

EXAMPLE 2. *Let ao1 and ao2 be specified as same as those in Example 1, the following access control policies can be articulated:*

$\boldsymbol{P1}$: $(<GP,\{h2\}>,\ ao1,\ \{treatment\},\ permit)$;

$\boldsymbol{P2}$: $(<SP,\{h2\}>,\ ao2,\ \{treatment, research\},\ permit)$; *and*

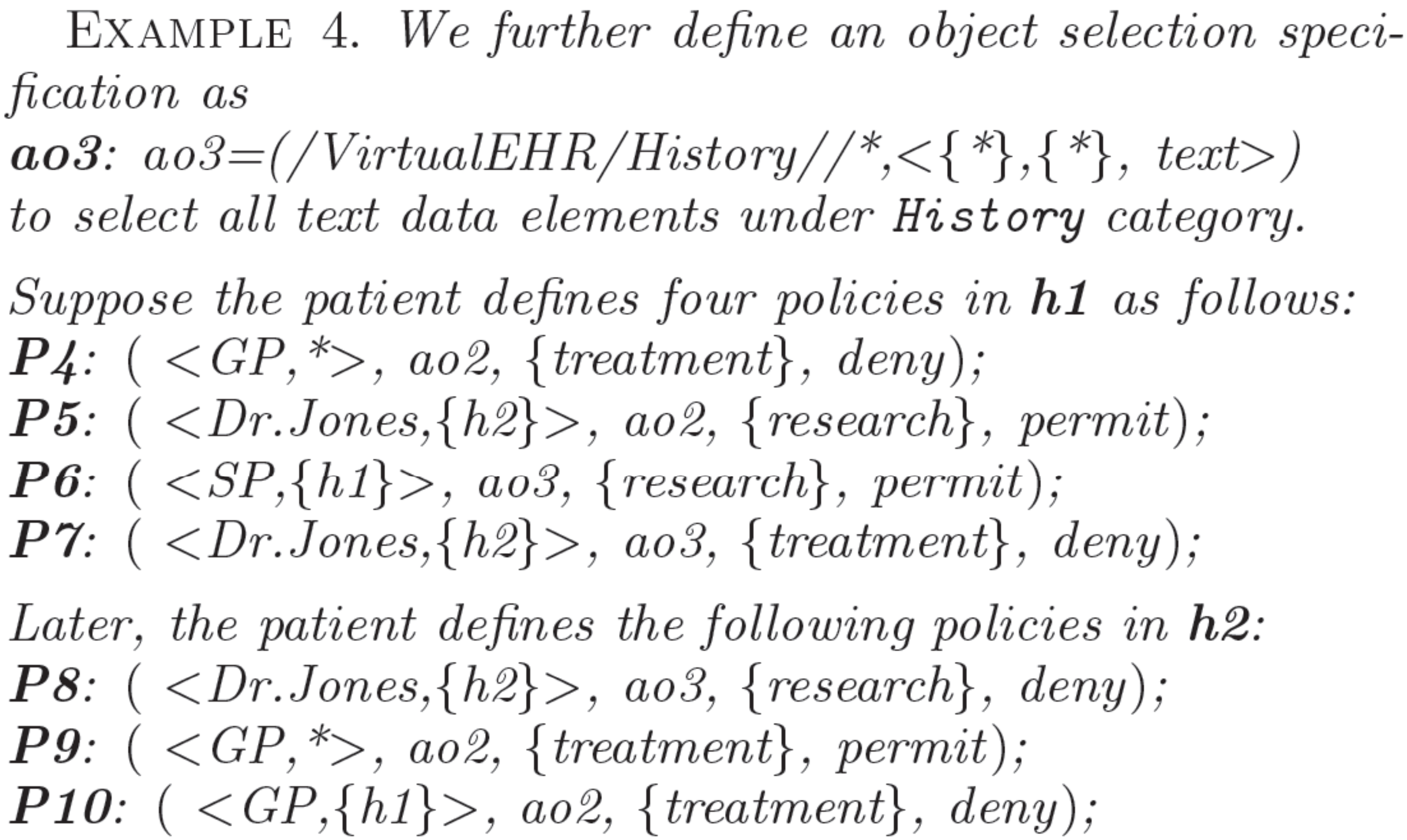
$\boldsymbol{P3}$: $(<Dr.\ Jones,\{h2\}>,\ ao2,\ \{treatment, research\},\ deny)$.

EXAMPLE 3. *The default policy and BG policy can be specified as follows:*

$\boldsymbol{P}_{D}$:$(<HP,\{*\}>,(\{*\},\{*\},*),\{treatment,payment,HCO\},permit)$;

$\boldsymbol{P}_{BG}$:$(<ERStaff,\{*\}>,(\{*\},\{*\},*),\{treatment\},permit)$.

C. Policy Composition and Anomaly Analysis

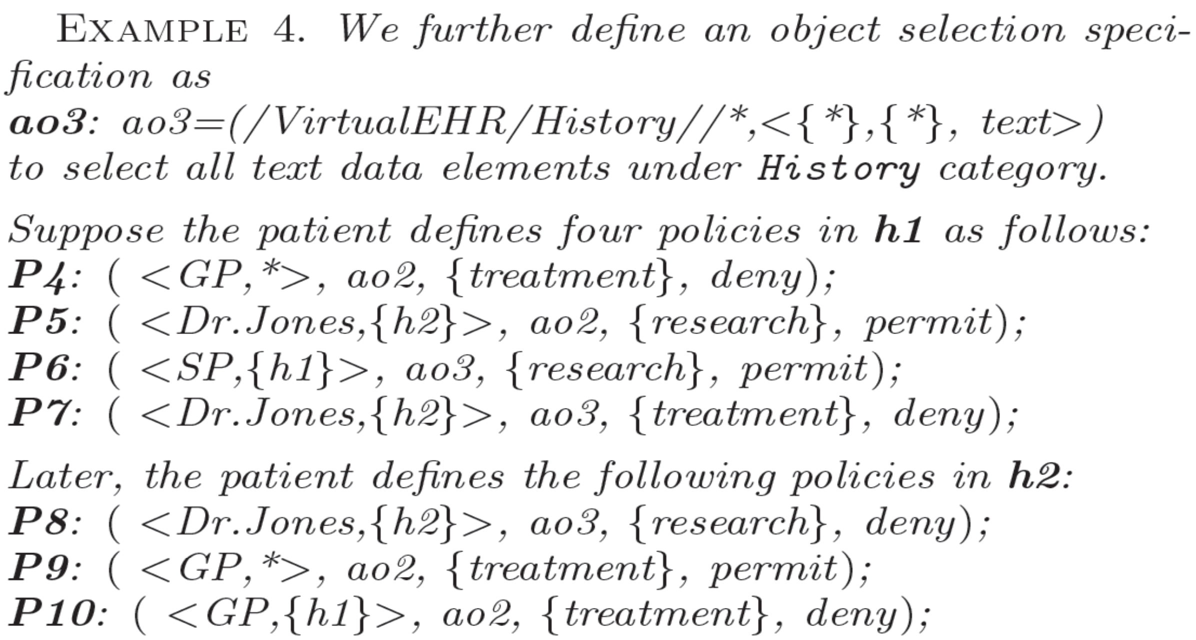


EXAMPLE 4. *We further define an object selection specification as*
ao3: ao3=(/VirtualEHR/History//*,<{*},{*}, text>)
to select all text data elements under `History` *category.*

Suppose the patient defines four policies in **h1** *as follows:*
P4: (<GP,*>, ao2, {treatment}, deny);
P5: (<Dr.Jones,{h2}>, ao2, {research}, permit);
P6: (<SP,{h1}>, ao3, {research}, permit);
P7: (<Dr.Jones,{h2}>, ao3, {treatment}, deny);

Later, the patient defines the following policies in **h2**:
P8: (<Dr.Jones,{h2}>, ao3, {research}, deny);
P9: (<GP,*>, ao2, {treatment}, permit);
P10: (<GP,{h1}>, ao2, {treatment}, deny);

Anomalies



EXAMPLE 4. *We further define an object selection specification as*
ao3*: ao3=(/VirtualEHR/History//*,<{*},{*}, text>)*
to select all text data elements under History *category.*

Suppose the patient defines four policies in ***h1*** *as follows:*
P4*: (<GP,*>, ao2, {treatment}, deny);*
P5*: (<Dr.Jones,{h2}>, ao2, {research}, permit);*
P6*: (<SP,{h1}>, ao3, {research}, permit);*
P7*: (<Dr.Jones,{h2}>, ao3, {treatment}, deny);*

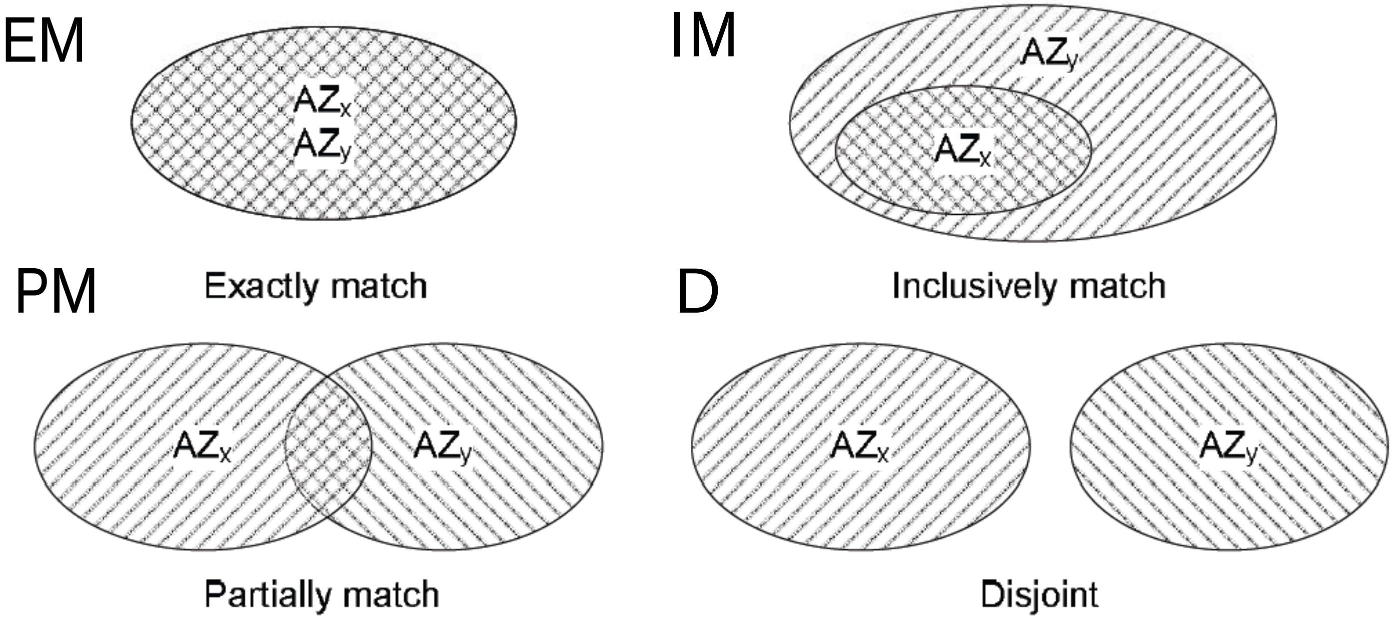
Later, the patient defines the following policies in ***h2****:*
P8*: (<Dr.Jones,{h2}>, ao3, {research}, deny);*
P9*: (<GP,*>, ao2, {treatment}, permit);*
P10*: (<GP,{h1}>, ao2, {treatment}, deny);*

Anomalies:

- Policy Inconsistency:
  - Contradictory (different effects only) (4,9)
  - Exception (different effects, sub) (6,8)
    - Suppose Dr. Jones is a Specialist in both H1 and H2
  - Correlation (different effects, intersect) (5,8)
    - Partial conflict
- Policy Inefficiency:
  - Redundancy (same, more general) (4,10)
  - Verbosity (different, merge) (7,8)

Patient-centric authorization model

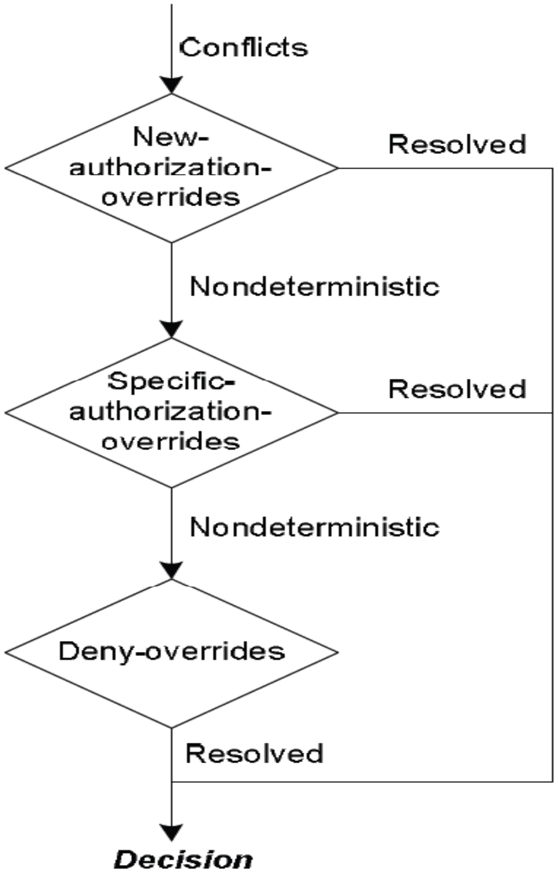
Authorization Zone



(EM or IM) and (same effect) = Redundancy
(EM) and (different effect) = Contradictory
(IM) and (different effect) = Exception
(PM) and (different effect) = Correlation
((PM) and (different effect)) or (D) = Normal

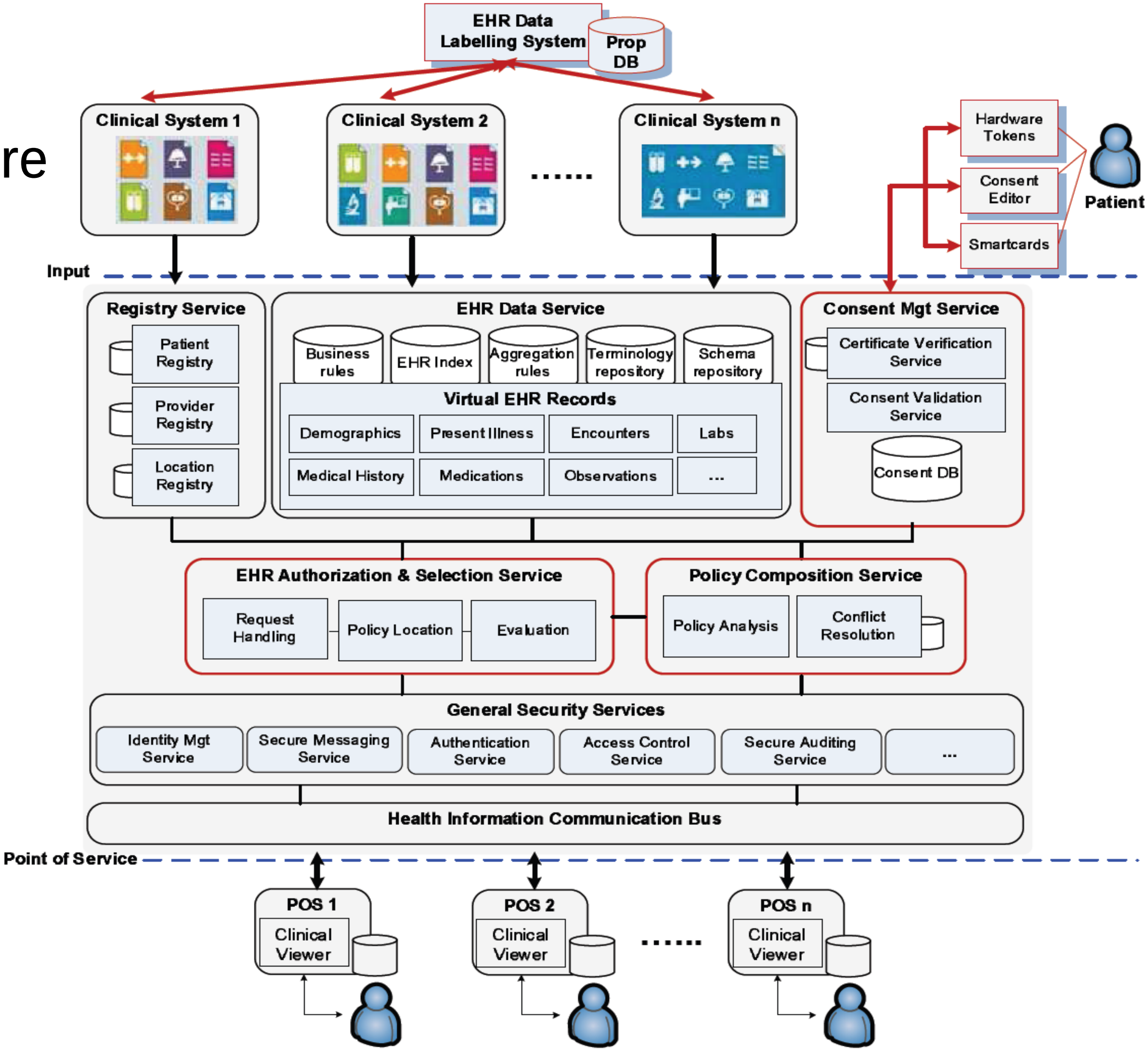
Patient-centric authorization model

Resolution



InfoShare

BG
General
Default



EHR Data Labelling System

Prop DB

Clinical System 1

Clinical System 2

......

Clinical System n

Hardware Tokens

Consent Editor

Smartcards

Patient

Input

Registry Service

Patient Registry

Provider Registry

Location Registry

EHR Data Service

Business rules

EHR Index

Aggregation rules

Terminology repository

Schema repository

Virtual EHR Records

Demographics	Present Illness	Encounters	Labs
Medical History	Medications	Observations	...

Consent Mgt Service

Certificate Verification Service

Consent Validation Service

Consent DB

EHR Authorization & Selection Service

Request Handling

Policy Location

Evaluation

Policy Composition Service

Policy Analysis

Conflict Resolution

General Security Services

Identity Mgt Service

Secure Messaging Service

Authentication Service

Access Control Service

Secure Auditing Service

...

Health Information Communication Bus

Point of Service

POS 1

Clinical Viewer

POS 2

Clinical Viewer

......

POS n

Clinical Viewer

(a) Overall System Architecture

Summary

- Patient centric
- Composite EHR
- Resolution rules
- Architecture

SAHI Project

- Privacy and HealthS&P
  - New Lab