

IS 2150 / TEL 2810

Introduction to Security

James Joshi
Professor, SIS



April 9/11, 2019

Security and Privacy in Healthcare



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; patient consent!
- 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

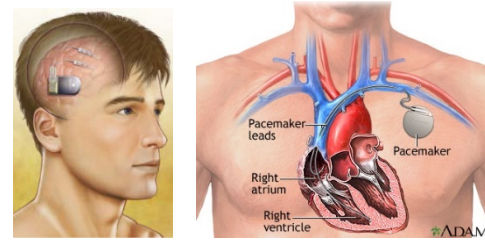


**Anytime, anywhere access to secure,
Privacy-aware Healthcare Services:
Issues, Approaches & Challenges**

Mohd. Anwar, James Joshi, Joseph Tan
(Health Policy and Technology Journal)



Continuous Monitoring and On-time intervention



in-body/out-body implantable/wearable devices, sensors

Anywhere, Anytime Personalized Healthcare/medicine

Enablers

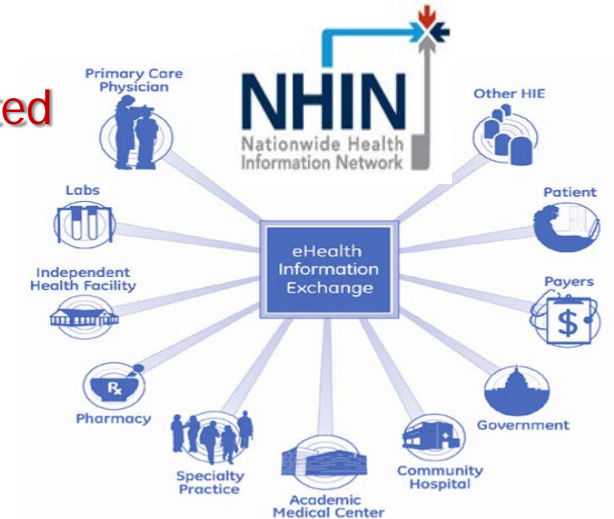
- Medical devices, IoT & Sensor technologies
- Mobile and Web technologies,
- Social networking, Cloud computing, Location based services
- Big Data analytics – AI, ML,

Many value added features/services

Social Support



Integrated Care



Self-care



mHealth App Spectrum



Simple

Complex



Single use mHealth

Focuses on a single purpose for a single user, typically consumer initiated:

- smartphone apps and wearable tech products that support the user to record data which may be communicated to others
- consumer driven, focus on wellness, diet and exercise.

Fitness tracker, weigh loss apps



Social mHealth

Draws upon the support and encouragement provided through social networks:

- gamification and competition based apps which encourage users to meet goals
- consumers likely to pursue activities independently.

Fitness tracker sharing via a SN



Integrated mHealth

Links apps and devices with the formal healthcare system:

- mobile technology linking patients and HCPs
- tailored to multiple end users: consumers, physicians and administrators.

Information from multiple apps that a patient uses is incorporated into the patients overall health record, giving a physician a more complete view



Complex mHealth

Leverages advanced, integrated analytics for decision support:

- predictive analytics applied to complex data generated through mHealth applications
- focus on achieving optimal management of a specific disease.

Source: Four Dimensions of Effective mHealth, Deloitte US Center for Health Solutions, 2014

Data mining using algorithms to analyze data collected via mobile devices to deliver insights on an individual's patterns of behavior for individual health management purposes. Data analysis oriented towards improving public health responses through analysis of sub-populations with different risk profiles and appropriate targeting of public health interventions

mHealth App market 10 takeaways



325,000 health apps

available in 2017

78,000 new health apps

added to major app stores in the last year

Android overtaking Apple

in numbers of available health apps

84,000 health app publishers

releasing apps

Gap of demand and supply widening

with high number of developers, low
downloads growth rates

\$5.4bn investment into digital health start-ups

fueling the market

3.6bn apps will be downloaded

by users in 2017 (estimated)

18% not developing health apps

due to uncertain regulations

Insurers are the #1 future distribution
channel

53% of digital health practitioners expect
health insurances to be future distribution
channel with best market potential

28% pure digital market players
in the digital health industry

Diverse mHealth publishers

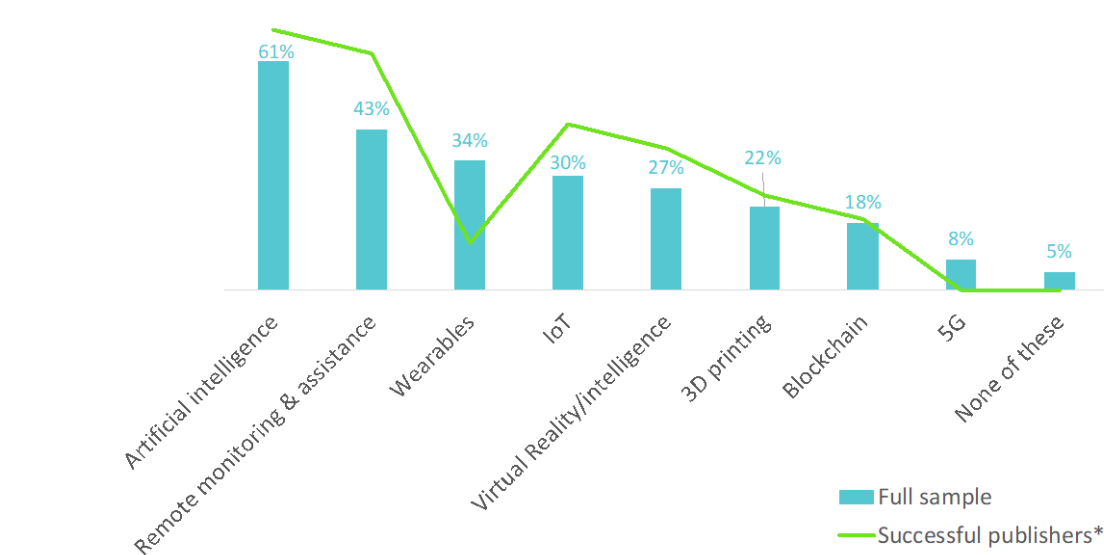
DIGITAL INTRUDERS: THE PURELY DIGITAL MARKET

Your organization is best described as:



AI SEEN AS THE MOST DISRUPTIVE TECHNOLOGY; SUCCESSFUL APP PUBLISHERS ARE GENERALLY MORE BULLISH ABOUT NEW TECHNOLOGIES

Most disruptive technologies to the data health sector within the next five years



*Successful publishers = >1M USD revenue and max 500 employees

Source: Research2Guidance - mHealth App Developer Economics study 2017 - n = 2,400

©Research2Guidance 2017



Source: Research2Guidance - mHealth App Developer Economics study 2017 - n = 2,400

©Research2Guidance 2017

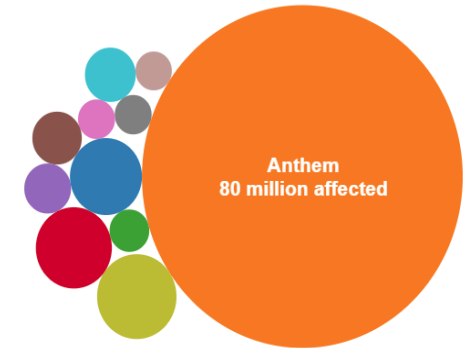
But ... Security & Privacy significant concerns

Privacy and Security are the most important concerns

Healthcare is a vulnerable industry

David Kotz et.al, "Privacy and Security in Mobile Health: A Research Agenda,"

Biggest healthcare data breaches



"57% of consumer .. report being skeptical of the overall benefits of health information technologies such as patient portals, mobile apps, and electronic health records mainly because of recently reported data hacking and a perceived lack of privacy protection by providers"



"The unwillingness of patients to comprehensively divulge all their medical information rose to 87 percent in the fourth quarter of 2016"



Alarming: Users are concerned " ... that their pharmacy prescriptions (90 percent), mental health notes (99 percent) and chronic condition (81 percent) data is being shared beyond their chosen provider and payer to retailers, employers, and or the government without their acknowledgement."

(as per a Black Book survey)

Security and Privacy Issues/Challenges

■ At-large

Enablers

- Medical devices, IoT & Sen
- Mobile and Web technolog
- Social networking, Cloud c
- Location based services
- Big Data analytics – AI, ML

Inherit all their

Leverage

Security & Privacy
Healthcare IT

HEALTHCARE CYBERSECURITY IS IN CRITICAL CONDITION

Severe Lack of Security Talent

The majority of health delivery orgs lack full-time, qualified security personnel

Legacy Equipment

Equipment is running on old, unsupported, and vulnerable operating systems.

Premature/Over-Connectivity

'Meaningful Use' requirements drove hyper-connectivity without secure design & implementation.

Vulnerabilities Impact Patient Care

One security compromise shut down patient care at Hollywood Presbyterian and UK Hospitals

Known Vulnerabilities Epidemic

One legacy, medical technology had over 1,400 vulnerabilities

Source: Healthcare Industry
Cybersecurity taskforce June 2017



Security and Privacy Issues/Challenges

Threat agents:

Insider OR *Outsider*

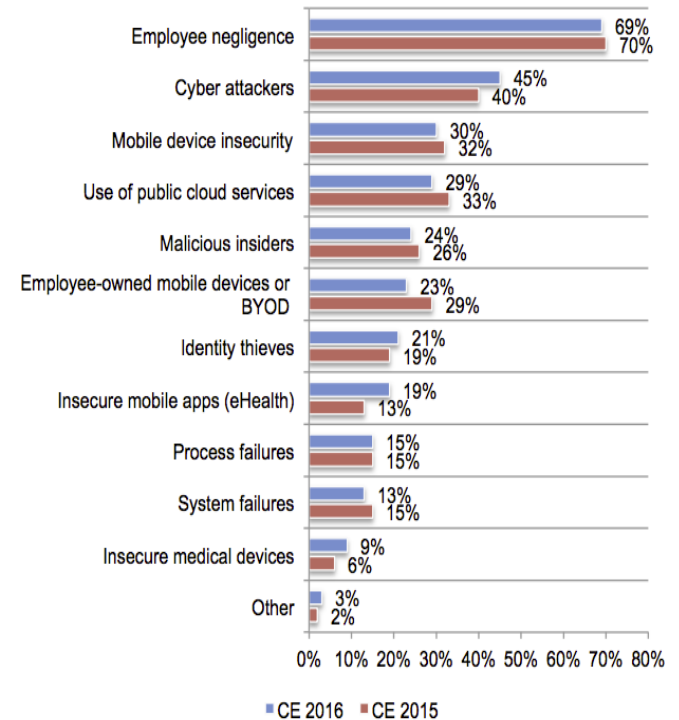
Attack sources by industry

1 January 2016 through 31 December 2016

Industry sector	% Malicious insider	% Inadvertent actor	% Outsiders
1 Financial services	5%	53%	42%
2 Information and communications	1%	3%	96%
3 Manufacturing	4%	5%	91%
4 Retail	2%	7%	91%
5 Healthcare	25%	46%	29%

Figure 9: Attack sources by industry – 1 January 2016 through 31 December 2016.

Figure 5. Security threats healthcare organizations worry about most
Three responses permitted





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 death 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

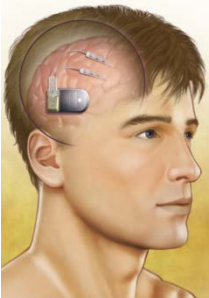
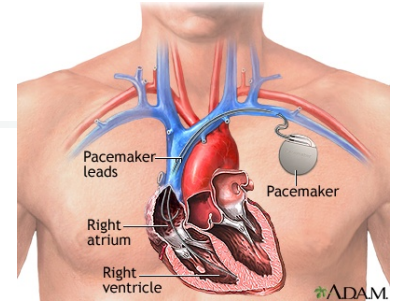
- Additional monitoring of environment is also important

- Katz's ADL (**Activities for Daily Living**: bathing, dressing, toileting,..) – for Geriatric 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 integrator
- Horizontal –
 - Among independent healthcare providers
 - 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.

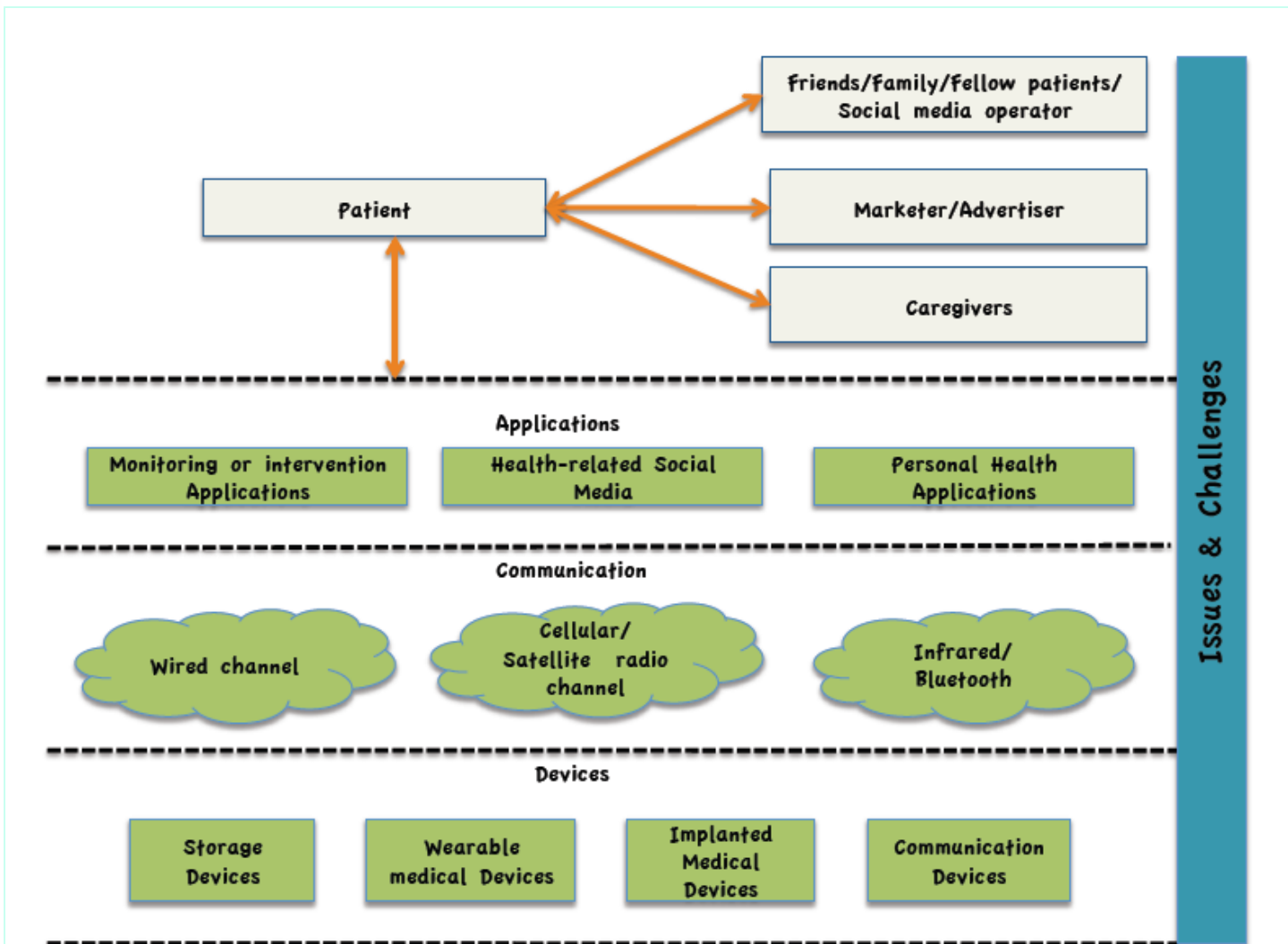


Social Support

- 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](https://www.youtube.com/watch?v=YfsRJWgwncU&feature=youtu.be)

Security and Privacy Issues/Challenges

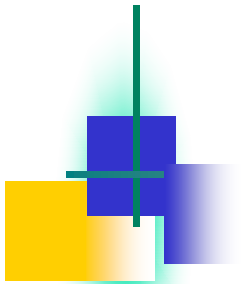


	Issues	Security problems	Approaches	Challenges
User Plane Demographics, Health condition, Physical ability, Mental ability	Demographic profiles and physical & mental abilities of patients are not the same.	- Attacks using non-technical and unintentional vulnerabilities - Targeted attacks on patients with certain characteristics	Human and social factor analysis	- Rich & diverse privacy & security requirements - Security solutions are challenged by human and social factors
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

Legacy / Mobile / Cloud Infrastructure

Epilepsy attacks
Phishing

Capture device id, location, demographic



HIPAA & HITECH



HIPAA

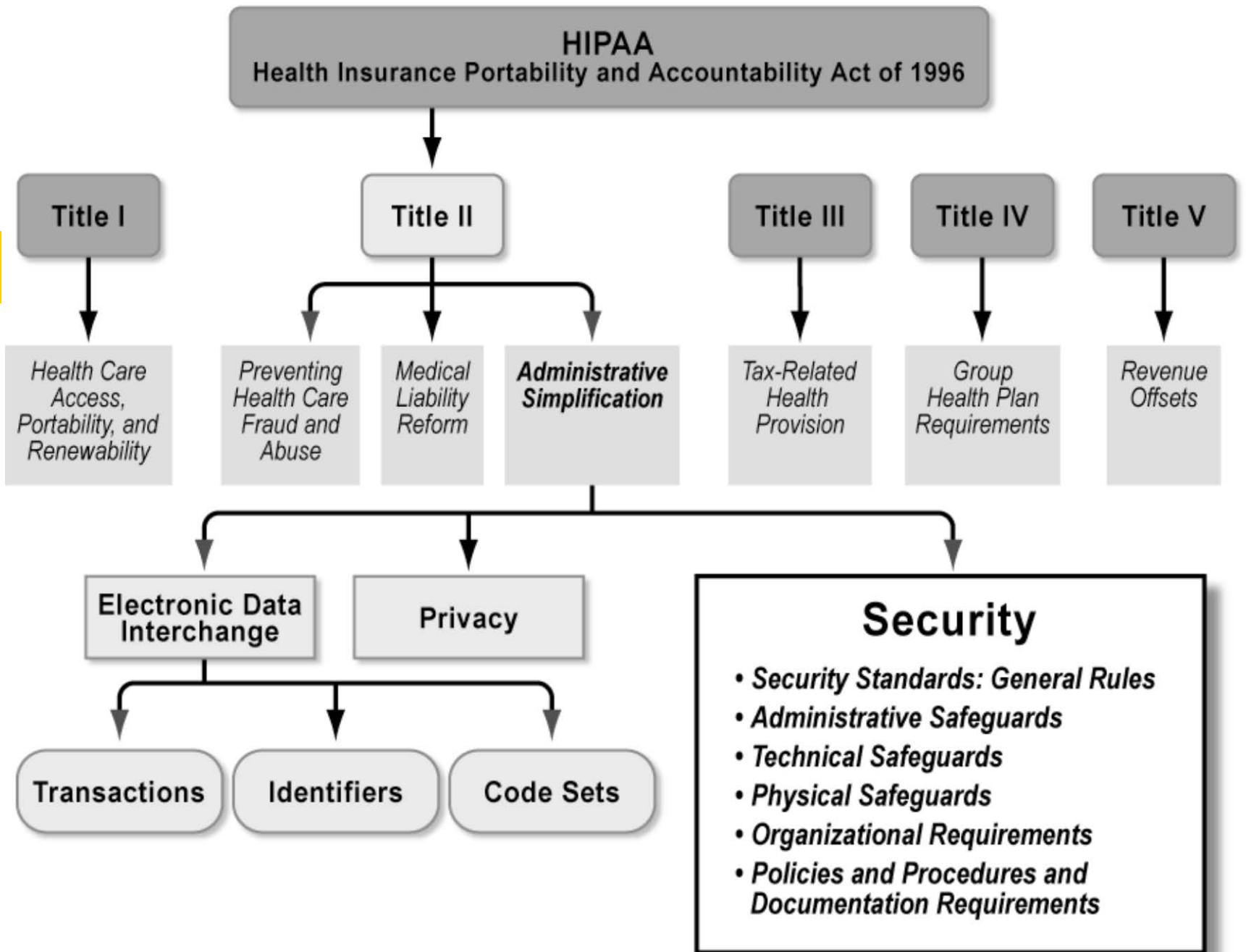
Health Insurance Portability & Accountability Act Of 1996 (HIPAA),

- also known as the Kennedy-Kassebaum Act
- **Protects confidentiality and security** of health care data by establishing and enforcing standards and standardizing electronic data interchange
- **Requires** organizations that retain health care information to use information **security mechanisms** to protect this information, as well as policies and procedures to maintain them
- Requires **comprehensive assessment** of organization's information security systems, policies, and procedures



HIPAA (Continued)

- Five fundamental privacy principles:
 - Consumer control of medical information
 - Boundaries on the use of medical information
 - Accountability for the privacy of private information
 - Balance of public responsibility for the use of medical information for the greater good measured against impact to the individual
 - Security of health information



CBS_01527a

Figure 1. HIPAA Components

HIPAA Rules

- **HIPAA Rules:** provide federal protections for patient health information held by *Covered Entities* (CEs) and *Business Associates* (BAs) and give patients an array of rights with respect to that information.
 - **Privacy Rule** -- protects the privacy of individually identifiable health information;
 - **Security Rule** -- sets national standards for the security of *electronic Protected Health Information* (ePHI); and
 - **Breach Notification Rule**-- requires CEs and BAs to provide notification following a breach of unsecured Protected Health Information (PHI).

CEs must comply with these.

BAs must comply with the HIPAA **Security Rule** and **Breach Notification Rule** as well as certain provisions of the HIPAA Privacy Rule.



Reading: Guide to Privacy and Security of Electronic Health Information

<https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf>



HIPAA

■ CEs include

- **Health care providers** who conduct certain standard administrative and financial transactions in electronic form,
- **Health plans:** Individual and group plans that provide or pay the cost of medical care
- **Health care clearinghouses:** entities that process nonstandard information they receive from another entity into a standard

A Health Care Provider	A Health Plan	A Health Care Clearinghouse
<p>This includes providers such as:</p> <ul style="list-style-type: none"> • Doctors • Clinics • Psychologists • Dentists • Chiropractors • Nursing Homes • Pharmacies <p>...but only if they transmit any information in an electronic form in connection with a transaction for which HHS has adopted a standard.</p>	<p>This includes:</p> <ul style="list-style-type: none"> • Health insurance companies • HMOs • Company health plans • Government programs that pay for health care, such as Medicare, Medicaid, and the military and veterans health care programs 	<p>This includes entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa.</p>



HIPAA: Business Associate

- **Privacy rule** - allows CEs to share to disclose PHI to BAs if they provide appropriate assurances
- BA is:
 - “person or entity, other than a workforce member (e.g., a member of your office staff), who performs certain functions or activities on your behalf, or provides certain services to or for you, when the services involve the access to, or the use or disclosure of, PHI.”
 - **BA functions or activities include:** claims processing, data analysis, quality assurance, certain patient safety activities, utilization review, and billing
 - **Examples:**
 - Health Information Organizations or Exchanges (HIOs/HIEs);
 - An entity that a CE contracts with to provide patients with access to a Personal Health Record (PHR) on behalf of a CE



Patients Rights under HIPAA

- Notice of privacy practices (NPP)
- Patient Access to Information (within 30 days of request)
- Amending Patient Information (within 60 days of request)
 - Can file “statement of disagreement”
- Accounting of Disclosures (limited)
 - Not needed for ones made for treatment, payment, operations and other purposes.
- Rights to Restrict Information (use and disclosure)
- Rights to confidential communications
 - Receive communications by means and from locations patients specify

Designated Record Set – is a group of records CE or BA maintains to make decisions about individuals (e.g., medical and billing records)



HIPAA Privacy Rule

- Privacy Rule
 - Protects most individually identifiable health information held by a CE and BA – called PHI (**Protected Health Information**) related to
 - Demographic information
 - The individual's past, present, or future physical or mental health or condition,
 - The provision of health care to the individual, or
 - The past, present, or future payment for the provision of health care to the individual.

Also - identifies the individual OR there is a reasonable basis to believe it can be used to identify the individual

List of 18 Identifiers

1. Names;
2. All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code, if according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
4. Phone numbers;
5. Fax numbers;
6. Electronic mail addresses;
7. Social Security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic, or code (note this does not mean the unique code assigned by the investigator to code the data)



HIPAA Privacy Rule

- Establishes national standards for the protection of certain health information.
- The Privacy Rule standards address
 - “the use and disclosure of PHI as well as standards for individuals’ privacy rights to understand and control how their health information is used and shared, including rights to examine and obtain a copy of their health records as well as to request corrections”
 - “limits Uses and Disclosures of Patient Information “
- Rules related to
 - Permitted Uses and Disclosures, etc. (Usage and Disclosure related)
 - Notice and Other Individual Rights
 - Administrative requirements – policies and procedures

(Check for more info: <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>)



HIPAA Security Rule

Establishes national set of minimum security standards for protecting all ePHI that a CE /BA create, receive, maintain, transmit.

Six main sections

- **Security standards: General Rules**

- general requirements all CEs must meet;
- establishes flexibility of approach;
- identifies standards and implementation specifications (both required and addressable);
- outlines decisions a CE must make regarding addressable implementation specifications; and
- requires maintenance of security measures to continue reasonable and appropriate protection of **electronic *protected health information***.
 - Ensure the confidentiality, integrity, and availability of ePHI that it creates, receives, maintains, or transmits;
 - Protect against any reasonably anticipated threats and hazards to the security or integrity of EPHI; and
 - Protect against reasonably anticipated uses or disclosures of such information that are not permitted by the [Privacy Rule](#).



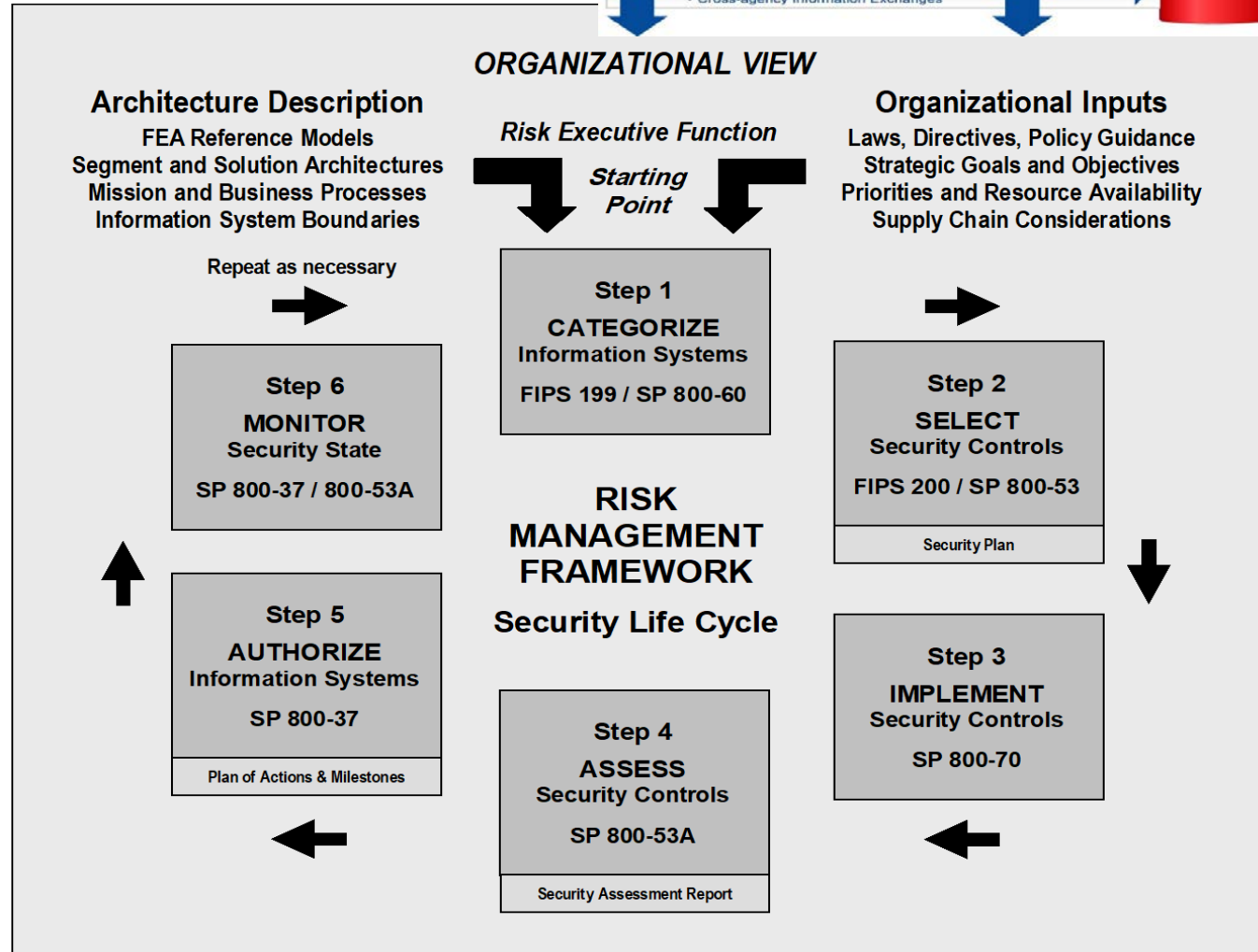
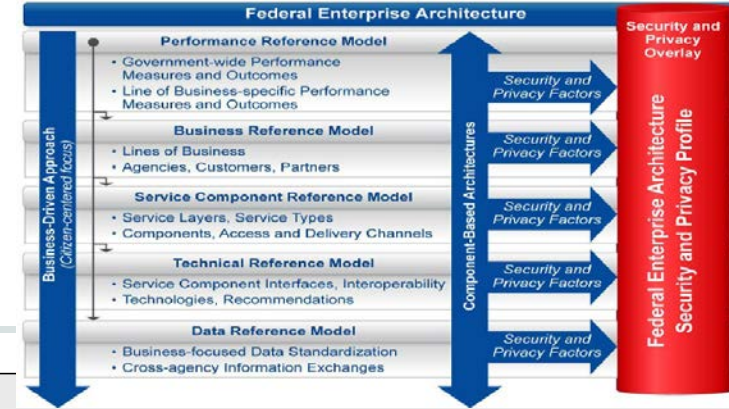
HIPAA Security Rule

- Administrative Safeguards
 - administrative actions and policies, and procedures to manage ...
- Physical Safeguards
 - physical measures, policies, and procedures ...
- Technical Safeguards
 - technology and the policy & procedures
- Organizational Requirements
 - standards for business associate contracts and other arrangements, including MoUs
- Policies and Procedures and Documentation Requirements
 - Requires implementation of reasonable and appropriate policies and procedures to comply with the standards, implementation ---
 - maintenance of written (which may be electronic) documentation and/or records that includes policies, procedures, actions, activities ...

NIST 800-66R1 on HIPAA

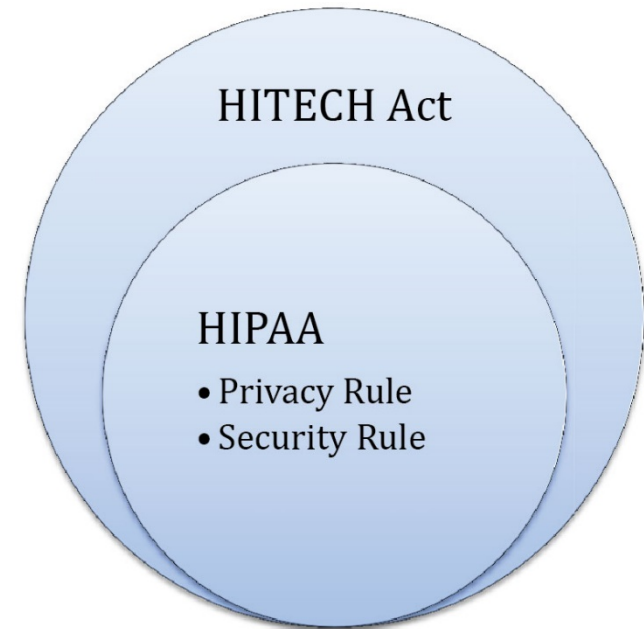
- HIPAA Security Rule is all about effective risk management
- Assessment, analysis of risk is foundation for CE compliance efforts

Can apply:
NIST-RMF



The American Recovery and Reinvestment Act (ARRA) of 2009

- After great recession!!
- Most significant changes
 - The final breach notification rule
 - Updates to business associate responsibilities
 - Expansion of penalty consequences
 - Investigative authority for potential violations to the Attorney General of each state

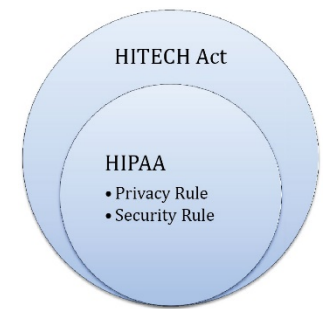


OCR

"The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, was signed into law on February 17, 2009, to promote the adoption and meaningful use of health information technology. Subtitle D of the HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules."

Strengthens HIPAA

HITECH Act



- Expands Administrative Simplification provision and added business associates to the list of those who are directly culpable for compliance to HIPAA
- OCR took control of enforcement of HIPAA vis the HITECH Act – dramatic effect
- HITECH requires
 - Business associate to implement each of the CIA safeguards under the HIPAA Security Rule that already applied to covered entities
 - Also imposes new requirements for covered entities to limit disclosures of PHI “to the extent practicable” to limited data set or, if needed by the CEs, to the min necessary to accomplish the intended purpose
 - Also changes to HIPAA –
 - Providing individuals with right to obtain PHI in e-format,
 - Enhancing fines and penalties for breaches
 - Dramatically changes the definition of “breach” as – an acquisition, access, or disclosure of unsecured PHI that is not otherwise permitted under HIPAA that compromises the security and privacy of PHI



HITECH Act

- HIPAA Beach Notification – did not exist prior to HITECH Act
 - One of the most drastic change!!
 - Any breach that impacts 500 or more individuals – needs to be reported
- Scope of CEs also clarified to include business associates such as
 - Billing providers
 - Health information exchanges
 - Software companies
 - Cloud computing providers
 - In some cases Banks
- Safe harbor in HITECH for encrypted info
 - If the info breached was encrypted with certified FIPS 140-2 encryption – the breach does not have to be reported
- Provides funding for auditors to review the security practices of covered entities in US



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."

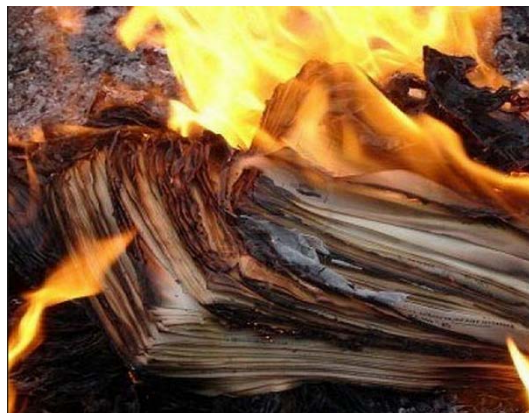


Why EHR?

Paperless.



Safe(?).



Readable.



Access anywhere.



Sharing Electronic Health Records

Treatment

scattered



Integrated, unified

Research, Study



Patient-centric Authorization

Not **user**, but **owner** controls the access to data!

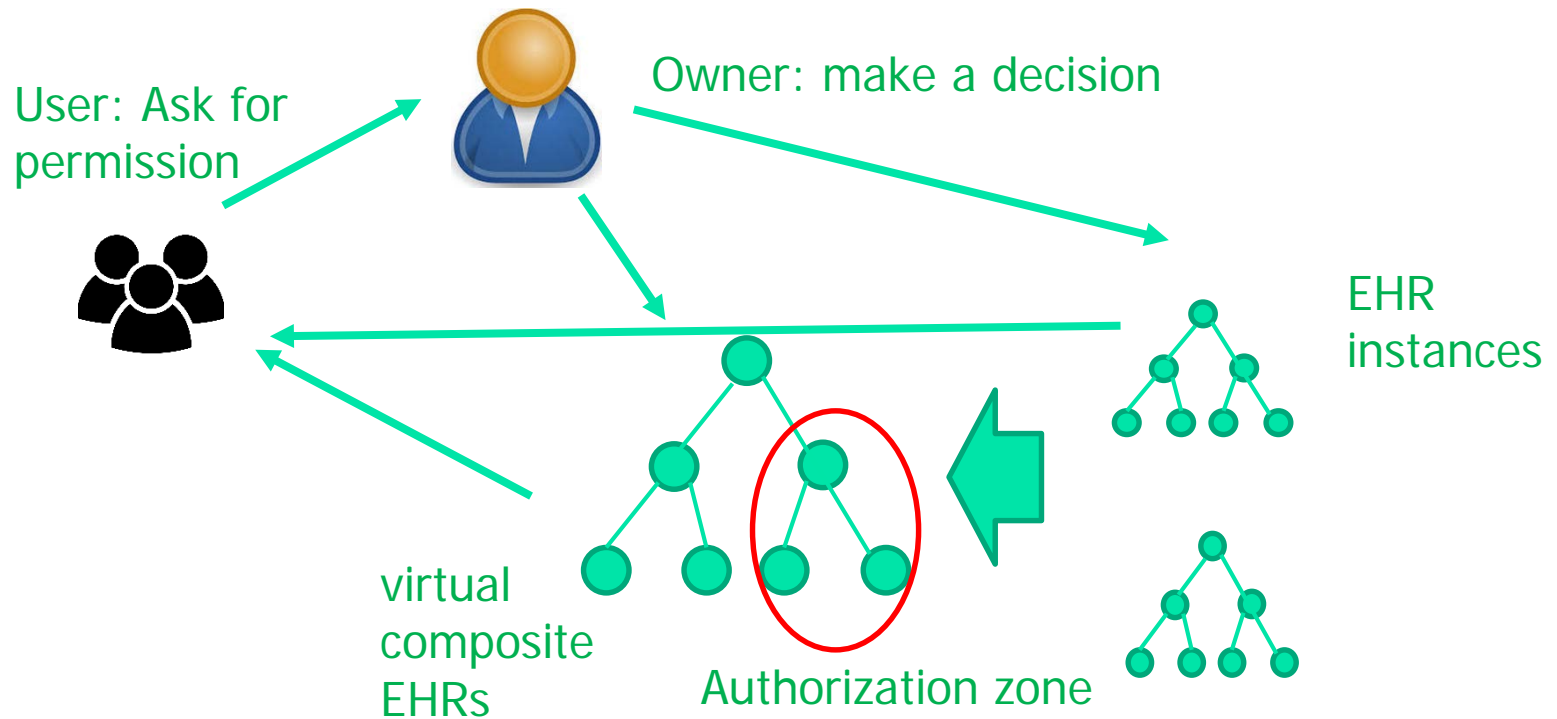
Why **owner**?

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.



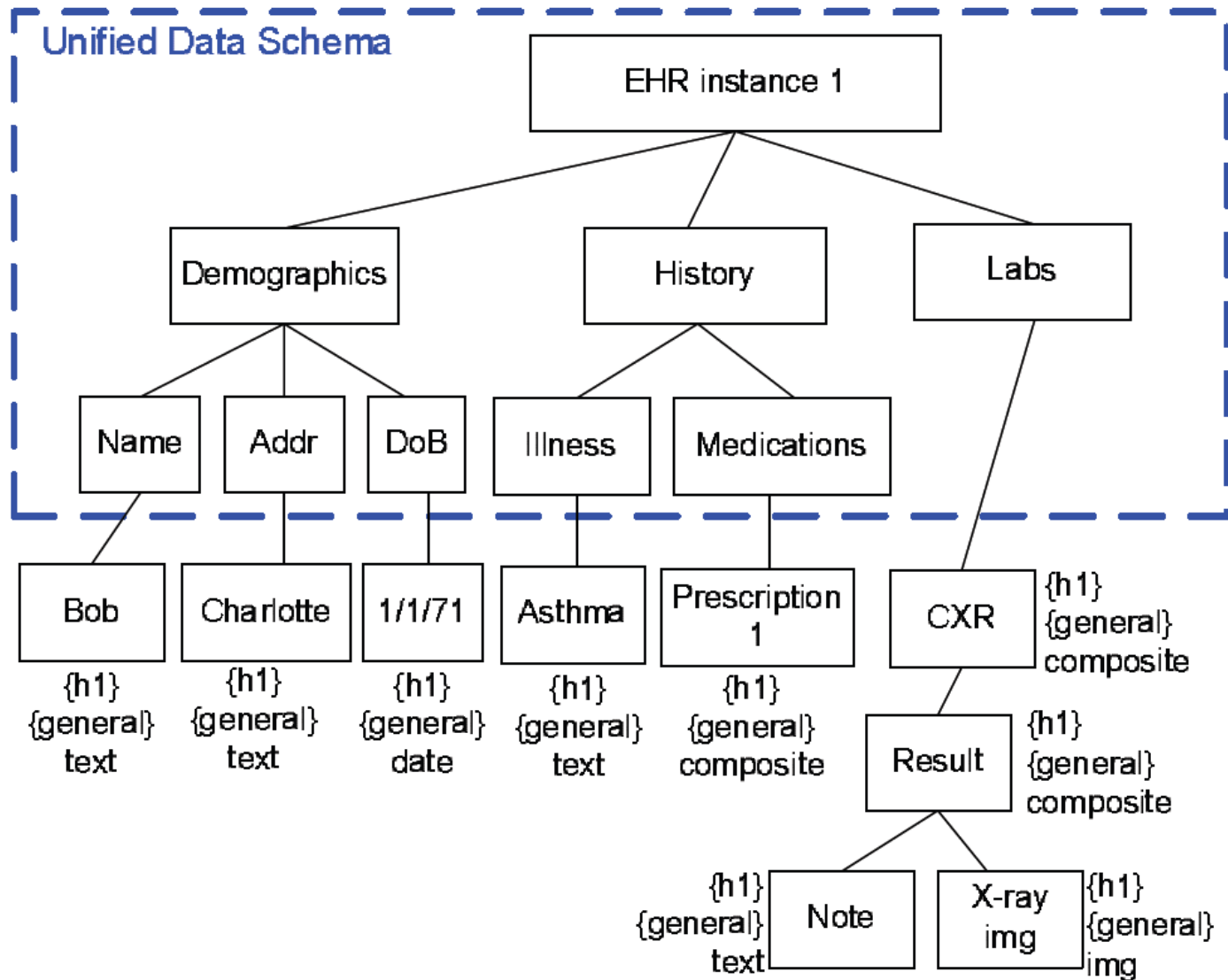
Patient-centric authorization model

Unified Logical EHR Model

A. Understand the model

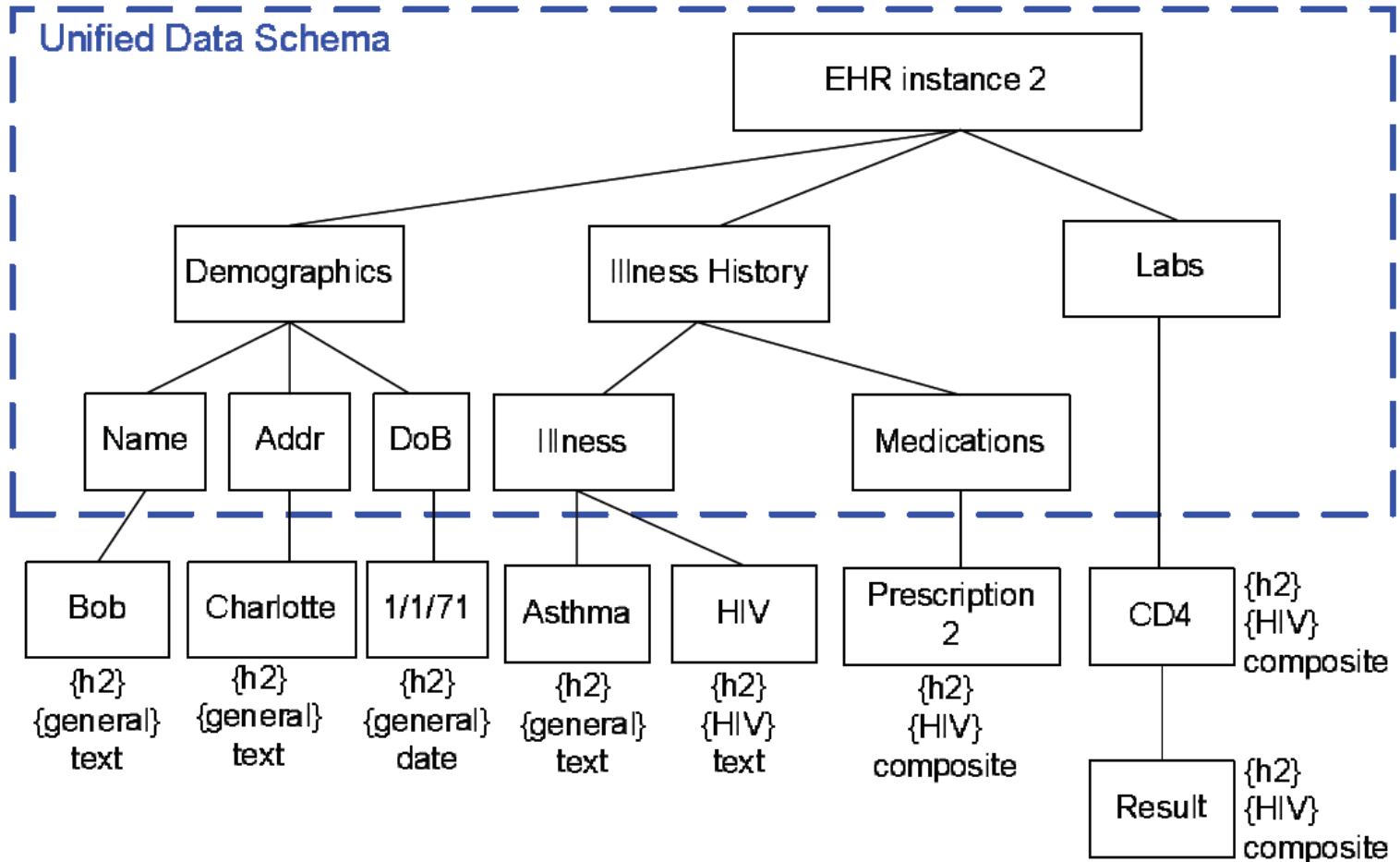
1. Unified Data Schema (UDS). (assumption)
2. Nodes.
3. Edges.
4. Properties. <origin, sensitivity, object type>

Patient-centric authorization model



a. EHR instance 1 (Hospital 1)

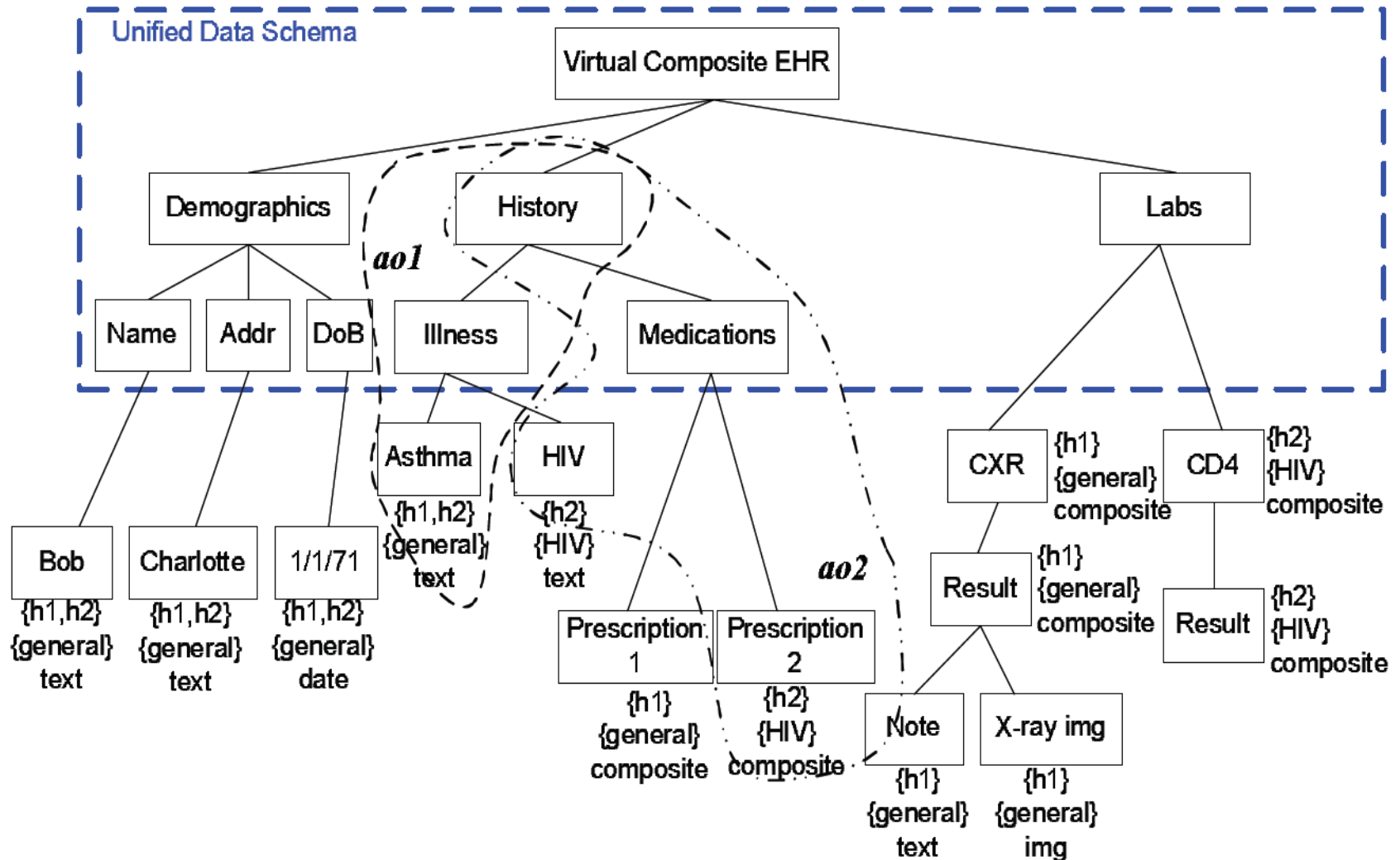
Patient-centric authorization model



b. EHR instance 2 (Hospital 2)

Patient-centric authorization model

Virtual Composite EHR





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 .

- $P_o = \{po_1, \dots, po_n\}$ is a collection of origin sets, where $po_i \subseteq O$ is a set of origins associated with a node, $i \in [1, n]$;
- $P_s = \{ps_1, \dots, ps_n\}$ 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

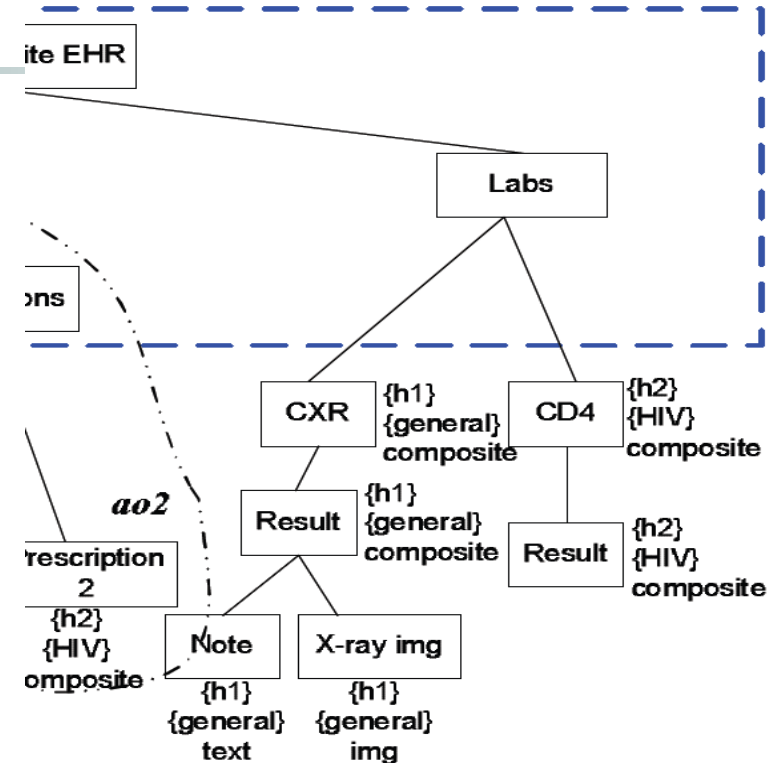


Table 1: Path Expression for Node Selection

Expression	Description	Example
<i>nodename</i>	Select the named nodes	<i>CXR</i>
/	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 $sub = \langle e, so \rangle$ or $sub = \langle r, so \rangle$, 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 $prop = \langle po, ps, pt \rangle$, 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.

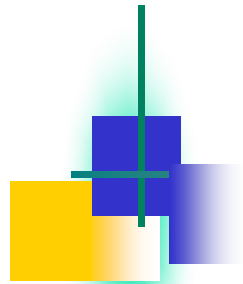
DEFINITION 5. (*Property Match*). Suppose $prop = \langle po, ps, pt \rangle$ is a filtration property specification, and $p' = (po', ps', t')$ is the property label of a node, the node matches the filtration property if the following conditions are satisfied:

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



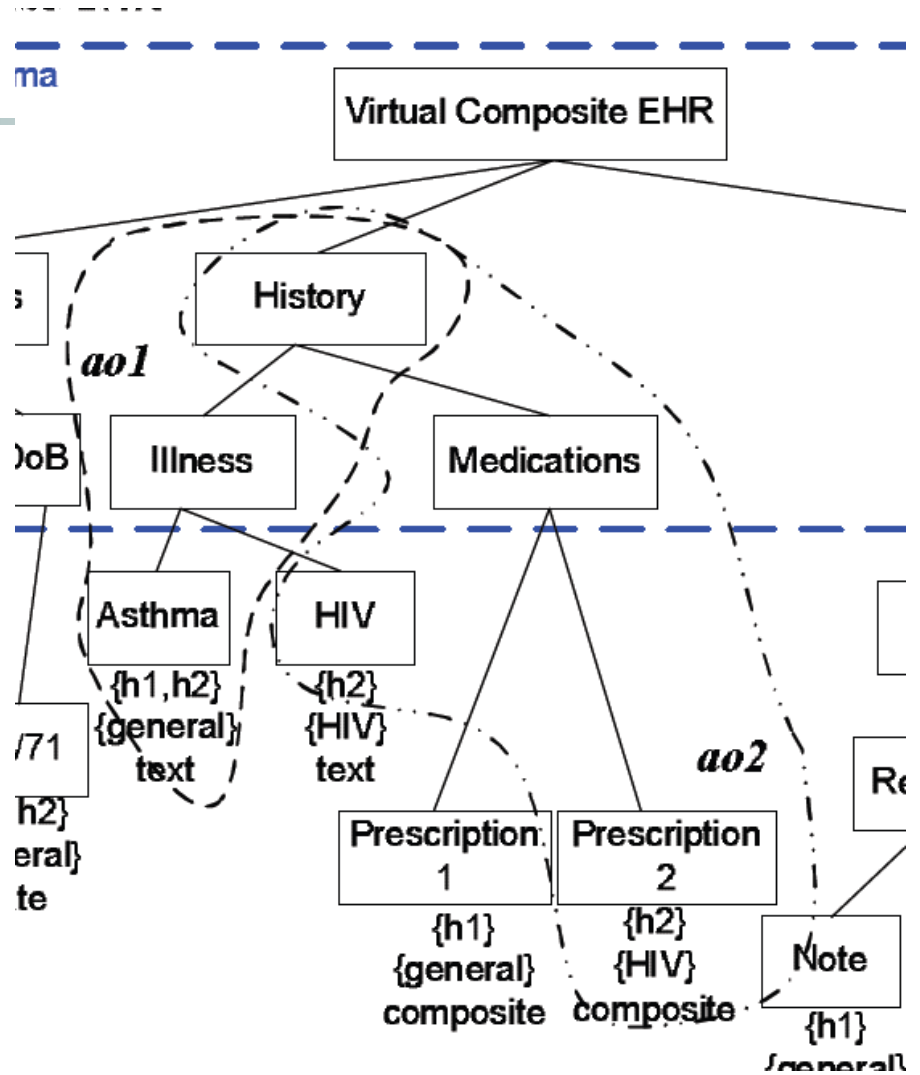
6. Object Specification.

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.

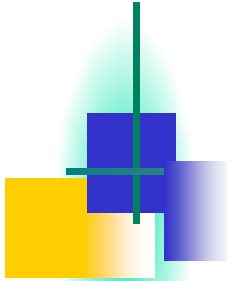
DEFINITION 7. (*Intended Purpose*). Let P be a set of purposes for business practices in healthcare domain. And let m be the total number of authorizations in the system. The intended purpose set $P_p = \{pp_1, \dots, pp_m\}$ is a collection of possible intended purpose sets, where $pp_i \subseteq P$ 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 $acp = \langle sub, ao, pp, effect \rangle$, 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:

$P1: (\langle GP, \{h2\} \rangle, ao1, \{treatment\}, permit);$

$P2: (\langle SP, \{h2\} \rangle, ao2, \{treatment, research\}, permit);$ and

$P3: (\langle Dr. Jones, \{h2\} \rangle, ao2, \{treatment, research\}, deny).$

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

$P_D: (\langle HP, \{*\} \rangle, (\{*\}, \{*\}, *), \{treatment, payment, HCO\}, permit);$

$P_{BG}: (\langle ERStaff, \{*\} \rangle, (\{*\}, \{*\}, *), \{treatment\}, permit).$



C. Policy Composition and Anomaly Analysis

EXAMPLE 4. We further define an object selection specification as

ao3: $ao3 = (/VirtualEHR/History//*, \langle \{*\}, \{*\}, text \rangle)$
to select all text data elements under *History* category.

Suppose the patient defines four policies in **h1** as follows:

P4: $(\langle GP, * \rangle, ao2, \{treatment\}, deny);$

P5: $(\langle Dr.Jones, \{h2\} \rangle, ao2, \{research\}, permit);$

P6: $(\langle SP, \{h1\} \rangle, ao3, \{research\}, permit);$

P7: $(\langle Dr.Jones, \{h2\} \rangle, ao3, \{treatment\}, deny);$

Later, the patient defines the following policies in **h2**:

P8: $(\langle Dr.Jones, \{h2\} \rangle, ao3, \{research\}, deny);$

P9: $(\langle GP, * \rangle, ao2, \{treatment\}, permit);$

P10: $(\langle GP, \{h1\} \rangle, ao2, \{treatment\}, deny);$



Anomalies

EXAMPLE 4. We further define an object selection specification as

ao3: $ao3 = (/VirtualEHR/History//*, \langle \{*\}, \{*\}, text \rangle)$
to select all text data elements under *History* category.

Suppose the patient defines four policies in **h1** as follows:

P4: $(\langle GP, * \rangle, ao2, \{treatment\}, deny);$

P5: $(\langle Dr.Jones, \{h2\} \rangle, ao2, \{research\}, permit);$

P6: $(\langle SP, \{h1\} \rangle, ao3, \{research\}, permit);$

P7: $(\langle Dr.Jones, \{h2\} \rangle, ao3, \{treatment\}, deny);$

Later, the patient defines the following policies in **h2**:

P8: $(\langle Dr.Jones, \{h2\} \rangle, ao3, \{research\}, deny);$

P9: $(\langle GP, * \rangle, ao2, \{treatment\}, permit);$

P10: $(\langle GP, \{h1\} \rangle, ao2, \{treatment\}, deny);$

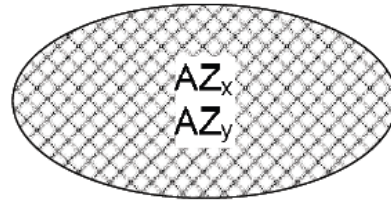
Anomalies:

- Policy Inconsistency:
 - Contradictory (different effects only) (4,9)
 - Exception (different effects, but one is subset of other) (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)

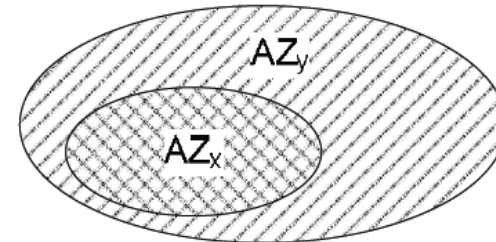
Patient-centric authorization model

Authorization Zone

EM

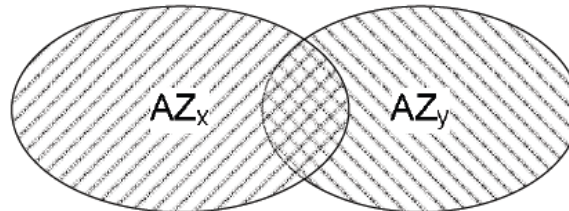


IM



PM

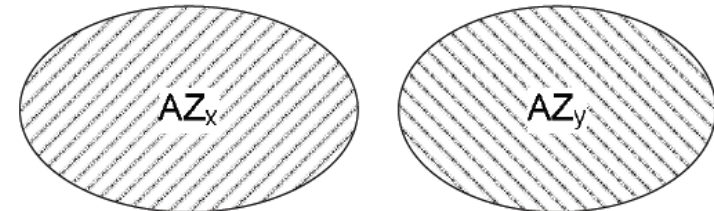
Exactly match



Partially match

D

Inclusively match



Disjoint

(EM or IM) and (same effect) = Redundancy

(EM) and (different effect) = Contradictory

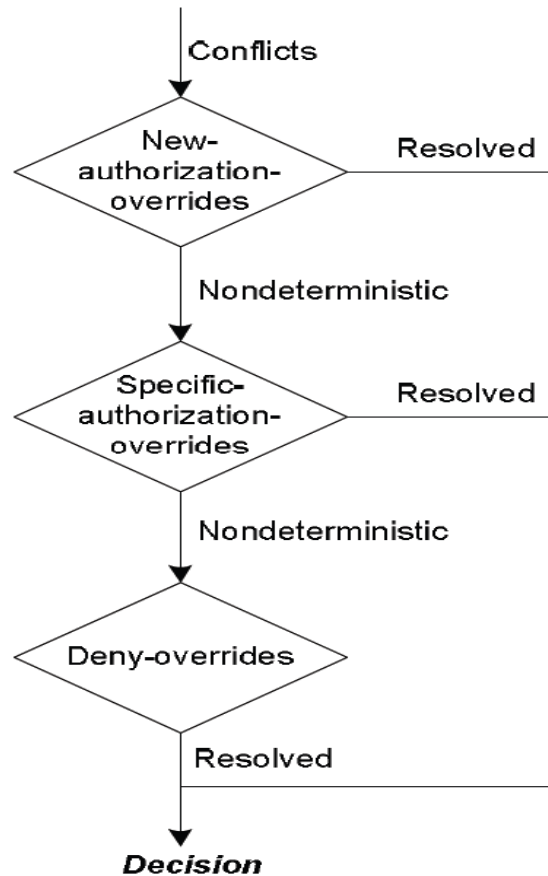
(IM) and (different effect) = Exception

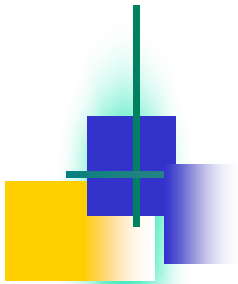
(PM) and (different effect) = Correlation

((PM) and (different effect)) or (D) = Normal

Patient-centric authorization model

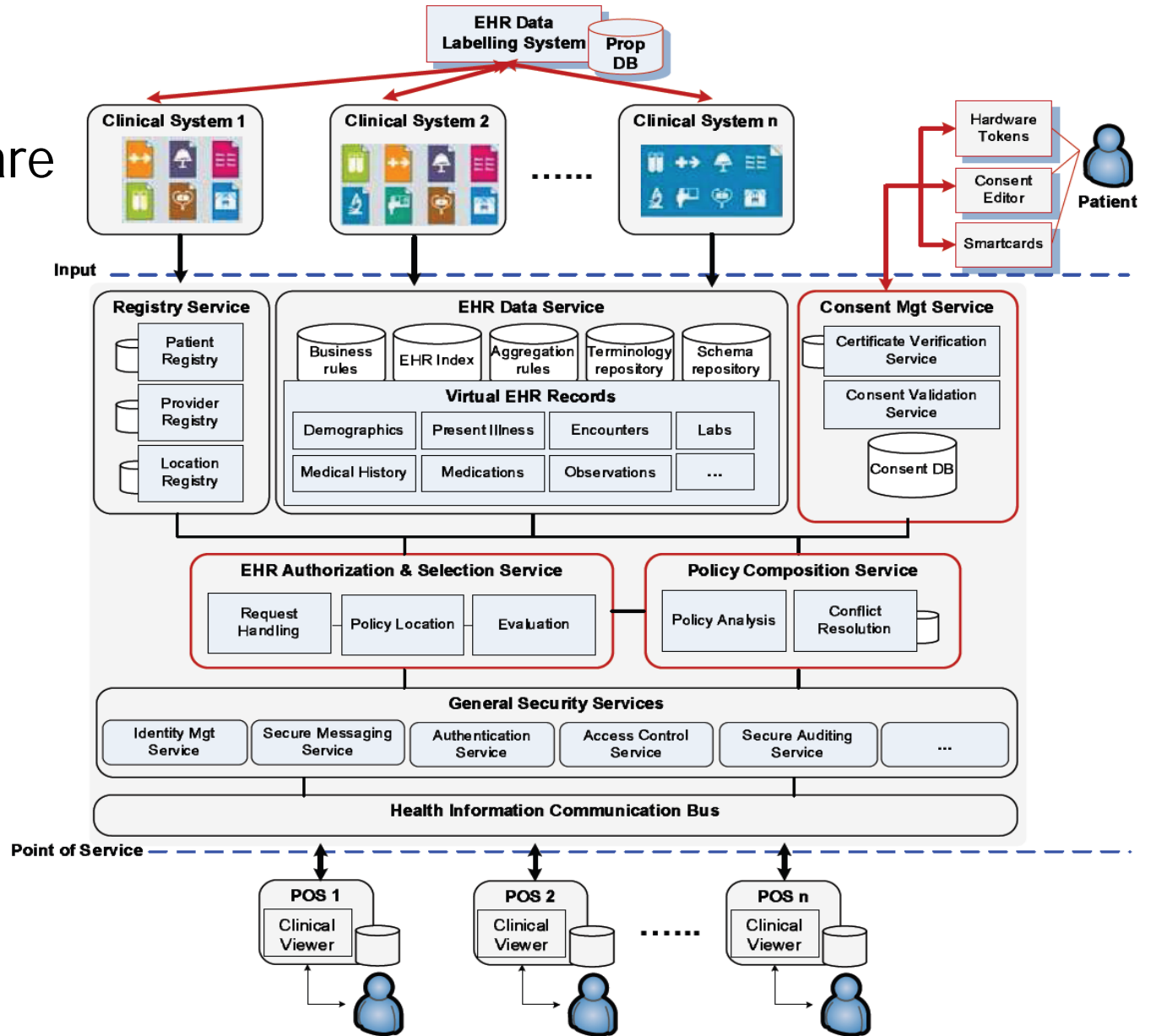
Resolution





InfoShare

BG
General
Default



(a) Overall System Architecture



Summary

- CISS policy derived from medical ethics and practices
- Anywhere, Anytime -- Security HealthCare IT Environment
- Patient centric, Composite HER, Resolution rules, Architecture