Webinar Series

HITSP

Healthcare Information Technology Standards Panel

Security, Privacy and Infrastructure (SPI)

Privacy is the goal – Security is the way

August 21, 2008 | 2:00 – 3:30 pm (Eastern)

Co-chairs, HITSP Security, Privacy and Infrastructure Technical Committee
John Moehrke, Enterprise Security Architect, GE Healthcare
Glen Marshall, Standards and Regulatory Manager, Siemens Healthcare

Sponsored by the HITSP Education, Communications and Outreach Committee

Learning Objectives

a webinar series on U.S. healthcare interoperability

- During this 90-minute webinar, participants will gain a basic knowledge of:
  - the core concepts related to security, privacy and infrastructure (SPI) needed for implementing interoperable Health Information Exchanges (HIEs), including privacy controls, security controls, identity and access controls, and audit controls;
  - the HITSP constructs developed to address SPI needs identified in Use Cases;
  - the core standards involved in the implementation of the HITSP SPI constructs;
  - examples of how the SPI constructs are being implemented in the marketplace.

Introduction: Steve's Story . . . part seven

- Patient is a 26-year-old male coping with the long-term effects of a brain tumor that was removed during his childhood
- Copies of patient's medical information can be found in the offices of doctors and specialists across the country
- Patient supports the development of a system where his information is available to the providers who need it
- However, patient wants assurances that only the doctors, technicians and healthcare providers that he gives permission to have access to components of his health records
  - i.e., a primary care physician needs to have access to everything, but administrators and technicians have access that is limited to their area of expertise
- Patient considers his medical history and health records a private matter that should be shared only on a need-to-know basis

Security and Privacy

- Medical records contain some of the most sensitive information about a person
- The privacy and security of health information are central to the doctor-patient relationship
- Many laws and regulations address the topic:
  - Federal: HIPAA, Privacy Act, Education Records Law, Mental Health Records Laws, Public Health Information Laws
  - State: There is a patchwork of varying types and levels of state privacy laws, though few address health privacy and security in a comprehensive fashion

Security and Privacy (continued)

- The Healthcare Information Technology Standards Panel (HITSP) focuses on Security and Privacy between entities, not within an entity

- Common Security and Privacy Constructs are used across the HITSP Interoperability Specifications

- **KEY BENEFIT**

  Organizations do **not** need to redo internal security procedures when implementing HITSP Interoperability Specifications

Infrastructure

- Most interoperability uses the same common types of mechanisms for exchanging information
- Instead of “reinventing the wheel” each time, common infrastructure constructs are reused
- Example
  - Many specifications use document sharing as a means of exchanging information
  - One of the Infrastructure Constructs is a Transaction Package called “Manage Sharing of Documents”
  - This Construct is used in many different Interoperability Specifications

Key Concepts

Privacy and Security of Health Information

- What is **privacy** (of health information)?
  - An individual's (or organization's) right to determine whether, when and to whom personal or organizational information is released.
  - The right of individuals to control or influence information that is related to them, in terms of who may collect or store it and to whom that information may be disclosed.

- What is **security** (of health information)?
  - A defined set of administrative, physical and technical actions used or taken to protect the confidentiality, availability and integrity of health information.

Key Concepts (continued)

SPI and Healthcare Information Interoperability

- **Security**

  Elements such as consistent time, secure communications channel, entity identity assertion, and others to protect health information systems and data

- **Privacy**

  Elements related to capturing and reporting patient's data disclosure consent directives electronically

- **Infrastructure**

  Structural elements of the exchange of health information, such as querying for existing data or notification of document availability

Key Concepts (continued)

SPI and Healthcare Information Interoperability

- **Confidentiality**
  - The property that data or information is not made available or disclosed to unauthorized persons or processes
- **Integrity**
  - The property that data or information has not been altered or destroyed in an unauthorized manner
- **Availability**
  - The property that data or information is accessible and usable upon demand by an authorized person

Key Terms – "Record"

Healthcare Information Interoperability

Electronic Medical Record (EMR)	Electronic Health Record (EHR)	Personal Health Record (PHR)
An electronic record of health-related information on an individual that can be created, gathered, managed and consulted by authorized clinicians and staff within one health care organization.	An electronic record of health-related information on an individual that conforms to nationally recognized interoperability standards and that can be created, managed and consulted by authorized clinicians and staff across more than one health care organization.	An electronic record of health-related information on an individual that conforms to nationally recognized interoperability standards and that can be drawn from multiple sources while being managed, shared, and controlled by the individual.

Source: National Alliance for Health Information Technology, Report to the Office of the National Coordinator for Health Information Technology – Defining Key Health Information Technology Terms, April 28, 2008

Key Terms – "Network"

Healthcare Information Interoperability

Health Information Exchange (HIE)	Health Information Organization (HIO)	Regional Health Information Organization (RHIO)
The electronic movement of health-related information among organizations according to nationally recognized standards.	An organization that oversees and governs the exchange of health-related information among organizations according to nationally recognized standards.	A health information organization that brings together health care stakeholders within a defined geographic area and governs health information exchange among them for the purpose of improving health and care in that community.

Source: National Alliance for Health Information Technology, Report to the Office of the National Coordinator for Health Information Technology – Defining Key Health Information Technology Terms, April 28, 2008

Building Policies

HITSP – enables / enforces

	Examples
International	OECD Guidelines on Transborder Flows
Country-Specific	US-HIPAA; EU-EC95/46; JP-Act 57 - 2003
Horizontal Industry	Medical Professional Societies
Enterprise	Backup and Recovery

Health Information Exchange (HIE)

Document based – HITSP Model

- Persistence
  - Captures the conclusion / summary of an episode
- Stewardship
  - Long term maintenance (patient's life 100+ years)
- Potential for Authentication
  - Which doctor's conclusion or opinion
  - What predicate data or knowledge
- Wholeness
  - Integrity, completeness, inclusive

Source: HL7 CDA

Privacy and Security Scenarios

- Prevent indiscriminate attacks (worms, Denial-of-service (DOS))
- Normal patient that accepts exchange of patient information
- Patient asks for accounting of disclosures
- Protect against malicious neighbor doctor
- Patient that retracts consent to publish
- Provider privacy
- Malicious data mining
- Access to emergency data set
- VIP (politician, movie star, sports figure)
- Domestic violence victim
- Daughter with sensitive tests hidden from parent
- Sensitive topics:
  mental health, sexual health
- Legal guardian (cooperative)
- Care-giver (assists w/ care)

HITSP SPI Constructs

Used across HITSP IS

SPI Constructs	IS01	IS02	IS03	IS04	IS05	IS06	IS07	ISXX
Privacy Controls								
Manage Consent Directives (TP30)	✓	✓	✓	✓	✓	✓	✓	✓
Security Controls								
Collect/Communicate Audit Trail (T15)	✓	✓	✓	✓	✓	✓	✓	✓
Consistent Time (T16)	✓	✓	✓	✓	✓	✓	✓	✓
Secured Communications Channel (T17)	✓	✓	✓	✓		✓	✓	✓
Identity and Access Control								
Entity Identity Assertion (C19)	✓	✓	✓	✓	✓	✓	✓	✓
Access Control (TP20)	✓		✓	✓	✓	✓	✓	✓

ISXX = Initial Assessment of Applicability of SPI Constructs to New 2008 Use Cases

HITSP SPI Constructs

Used across HITSP IS

SPI Constructs	IS01	IS02	IS03	IS04	IS05	IS06	IS07	ISXX
Privacy Controls								
Manage Consent Directives (TP30)	✓	✓	✓	✓	✓	✓	✓	✓
Security Controls								
Collect/Communicate Audit Trail (T15)	✓	✓	✓	✓	✓	✓	✓	✓
Consistent Time (T16)	✓	✓	✓	✓	✓	✓	✓	✓
Secured Communications Channel (T17)	✓	✓	✓	✓		✓	✓	✓
Identity and Access Control								
Entity Identity Assertion (C19)	✓	✓	✓	✓	✓	✓	✓	✓
Access Control (TP20)	✓		✓	✓	✓	✓	✓	✓

ISXX = Initial Assessment of Applicability of SPI Constructs to New 2008 Use Cases

TP 30 HITSP Manage Consent Directives

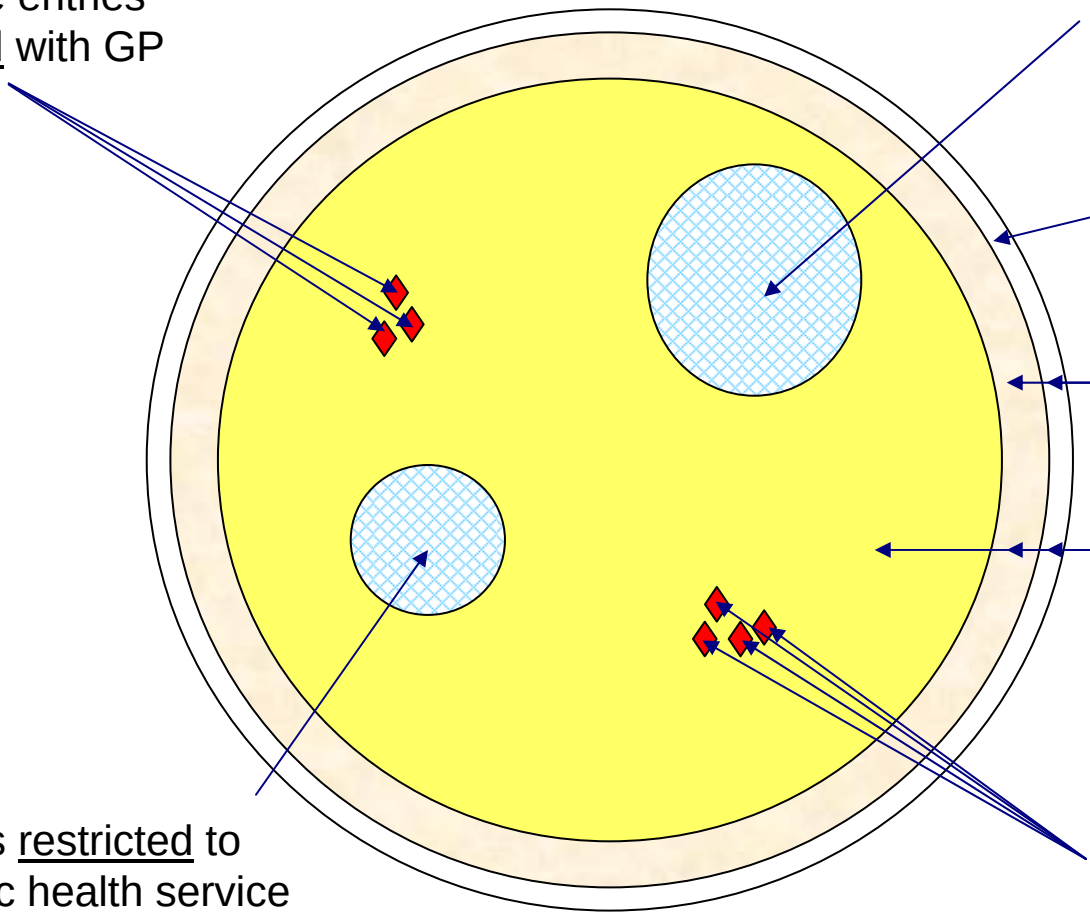
- Concept
  Manage Patient Consent choices

- Key Properties
  - Human Readable Consents
  - Machine Processable
  - Supports role-based access control (RBAC)

- Value Proposition
  - **RHIO/HIE**
    - Can develop and implement privacy policies with role-based or other access control mechanisms supported by edge/EHR systems
  - **Consumer**
    - Be made aware of an institution's privacy policies
    - Have an opportunity to selectively control access to their healthcare information

Example

Document accessibility



Source: Dipak Kalra & prEN 13606-4

Basic Consent (Opt-In and Opt-Out)

Enabling Role-Based Access Control (RBAC)

Entries accessible to clinical in emergency

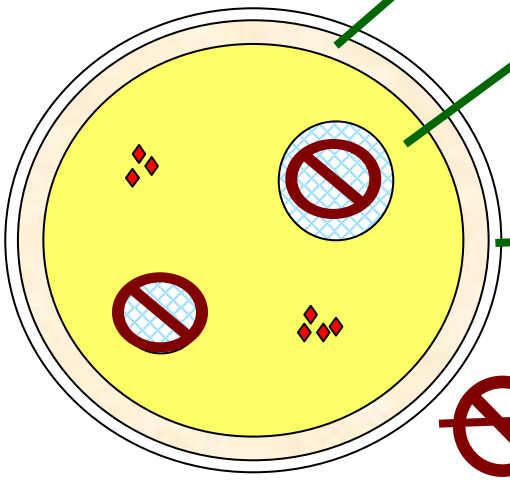
Entries accessible to direct care teams

Entries accessible to administrative staff

Entries accessible to research staff

Basic Consent

On an Episode Basis



Entries accessible to clinical in emergency

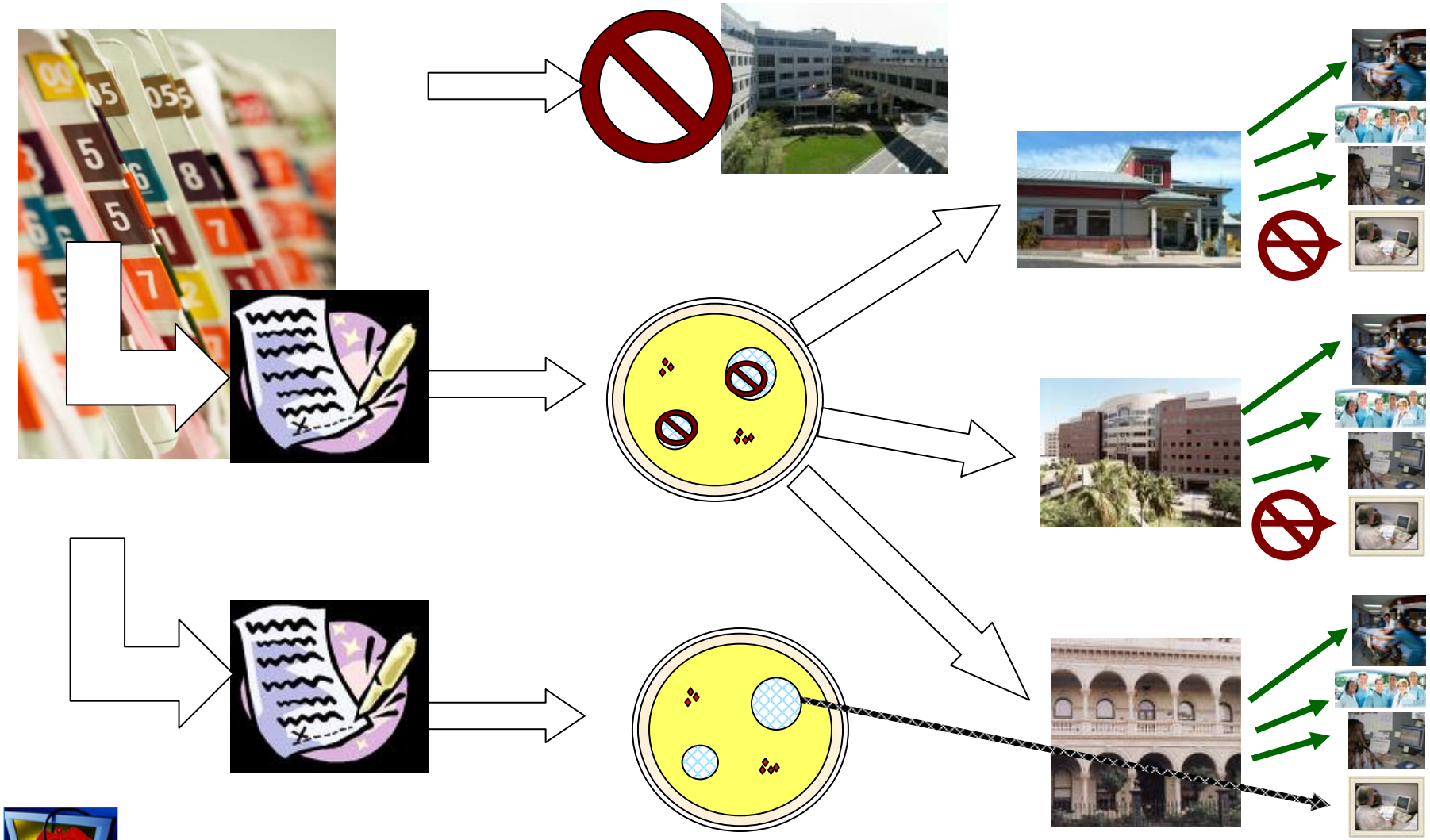
Entries accessible to direct care teams

Entries accessible to administrative staff

Entries accessible to research staff

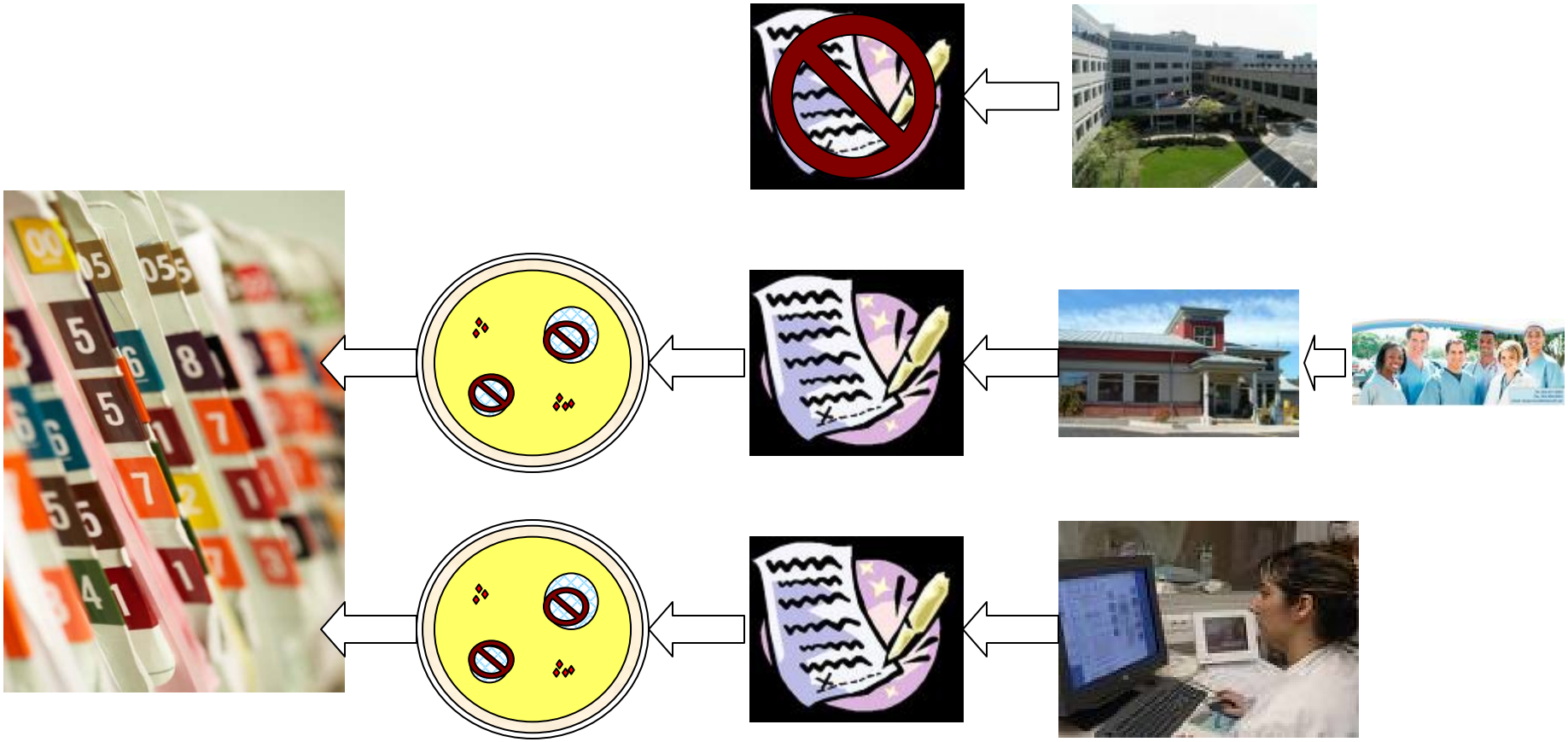
Basic Consent

Enabling Additional Access (e.g. Research)



Basic Consent

Publication Controls



HITSP SPI Constructs

Used across HITSP IS

SPI Constructs	IS01	IS02	IS03	IS04	IS05	IS06	IS07	ISXX
Privacy Controls								
Manage Consent Directives (TP30)	✓	✓	✓	✓	✓	✓	✓	✓
Security Controls								
Collect/Communicate Audit Trail (T15)	✓	✓	✓	✓	✓	✓	✓	✓
Consistent Time (T16)	✓	✓	✓	✓	✓	✓	✓	✓
Secured Communications Channel (T17)	✓	✓	✓	✓		✓	✓	✓
Identity and Access Control								
Entity Identity Assertion (C19)	✓	✓	✓	✓	✓	✓	✓	✓
Access Control (TP20)	✓		✓	✓	✓	✓	✓	✓

ISXX = Initial Assessment of Applicability of SPI Constructs to New 2008 Use Cases

Methods of Assuring Security

- Risk Assessment
  - Asset is the information in Registry & all Repositories
  - Confidentiality, integrity, and availability
  - Patient safety overrides privacy (when they conflict)
- Accountability
  - Access control model – Prevention
  - Audit control model – Reaction
- Policy Enforcement
  - Mutually agree to enforce policies
  - Enforcement of policies centrally

T 17 Secured Communication Channel

- Concept
  - To ensure the authenticity, integrity, and confidentiality of transactions, and the mutual trust between communicating parties
- Objectives
  - provide mutual node authentication to assure each node of the others' identity;
  - provide transmission integrity to guard against improper information modification or destruction while in transit; and
  - provide transmission confidentiality to ensure that information in transit is not disclosed to unauthorized individuals, entities, or processes

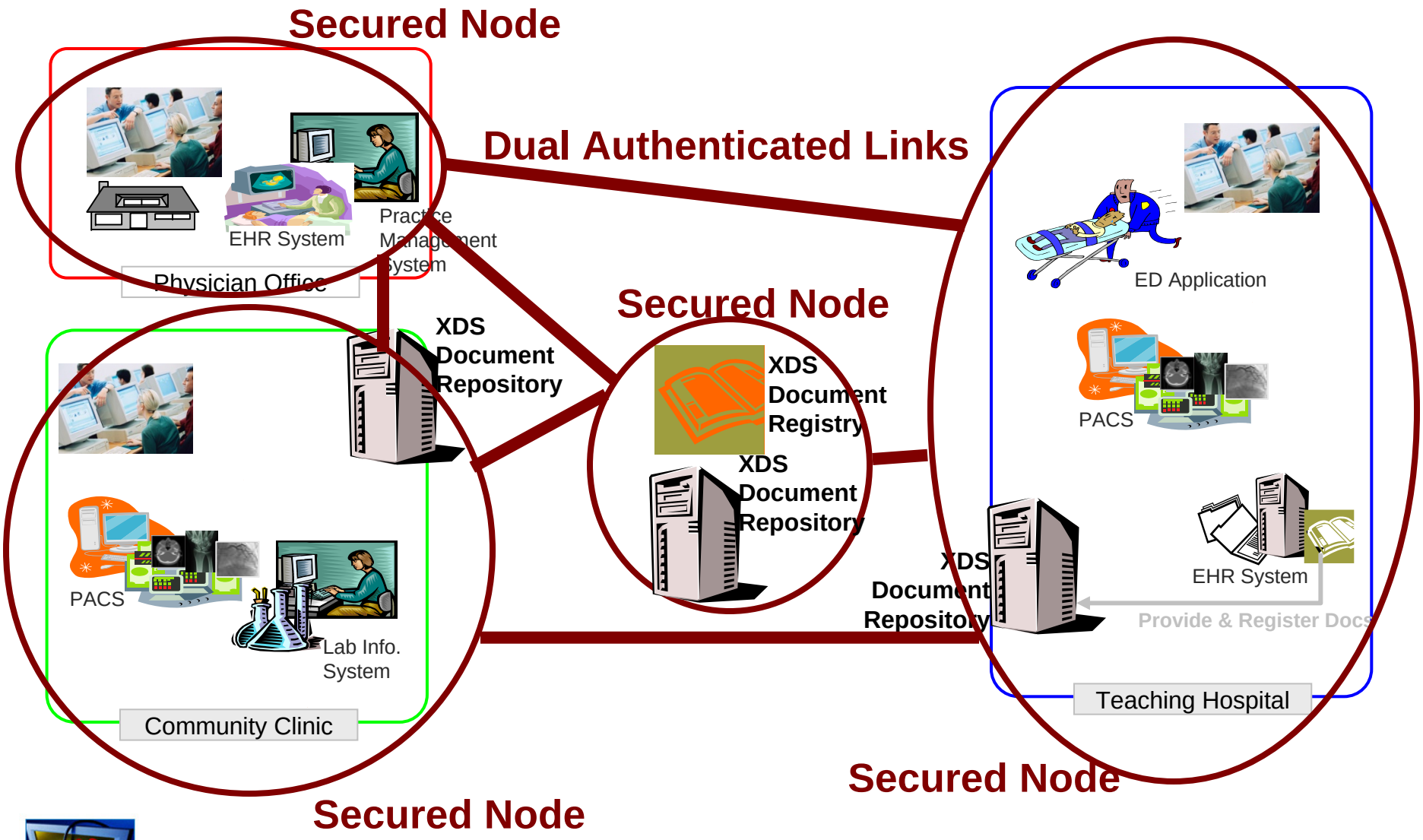
T 17 Secured Communication Channel (continued)

- Selected Composite Standards
  - IHE* Audit Trail and Node Authentication (IHE ATNA) Node Authentication

- Selected Base Standards
  - X.509 for digital certificates
  - RFC 2246 for bilateral authentication and encryption

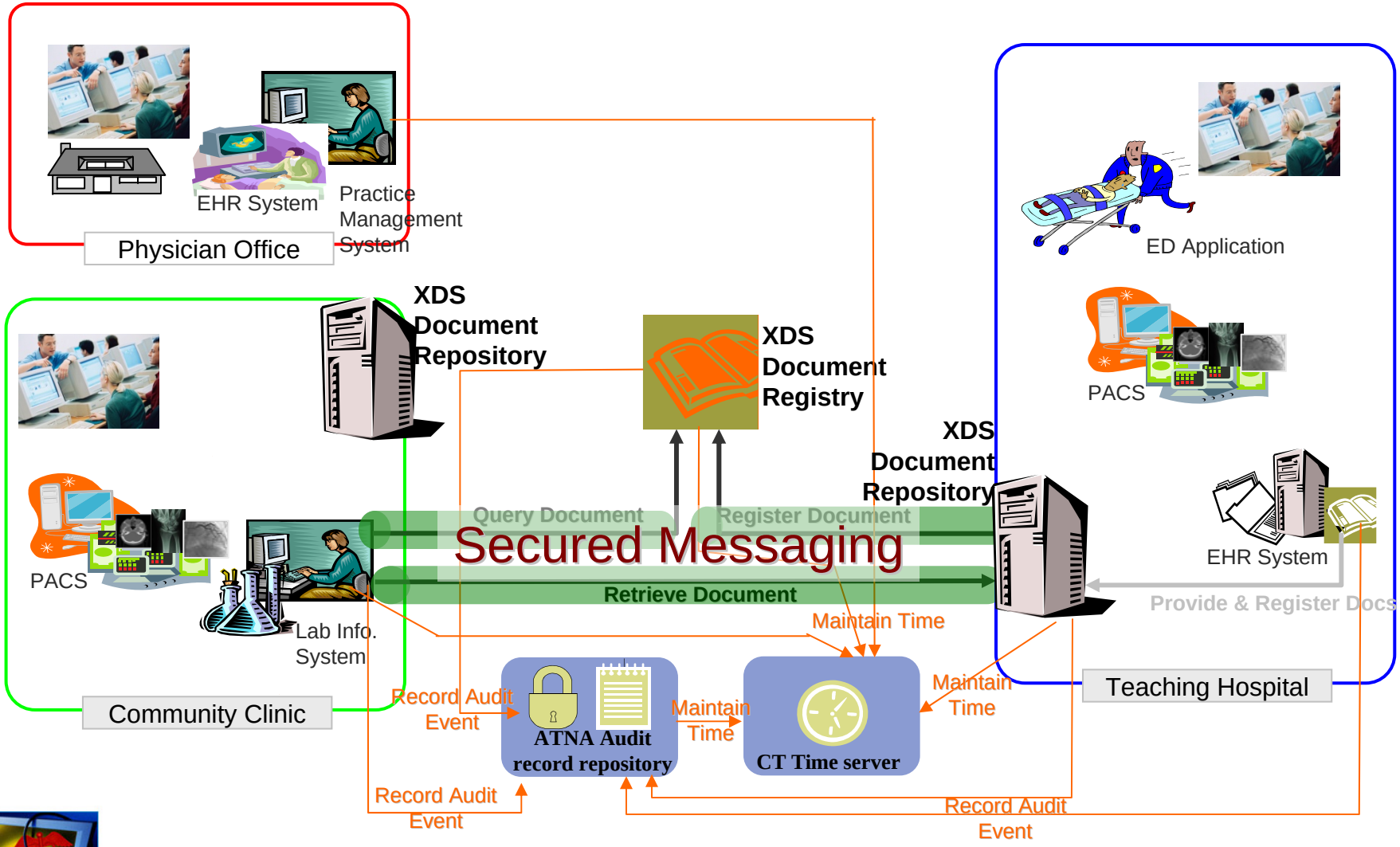
* IHE - Integrating the Healthcare Enterprise

T 17 Secured Communication Channel (continued)



T 16 Consistent Time

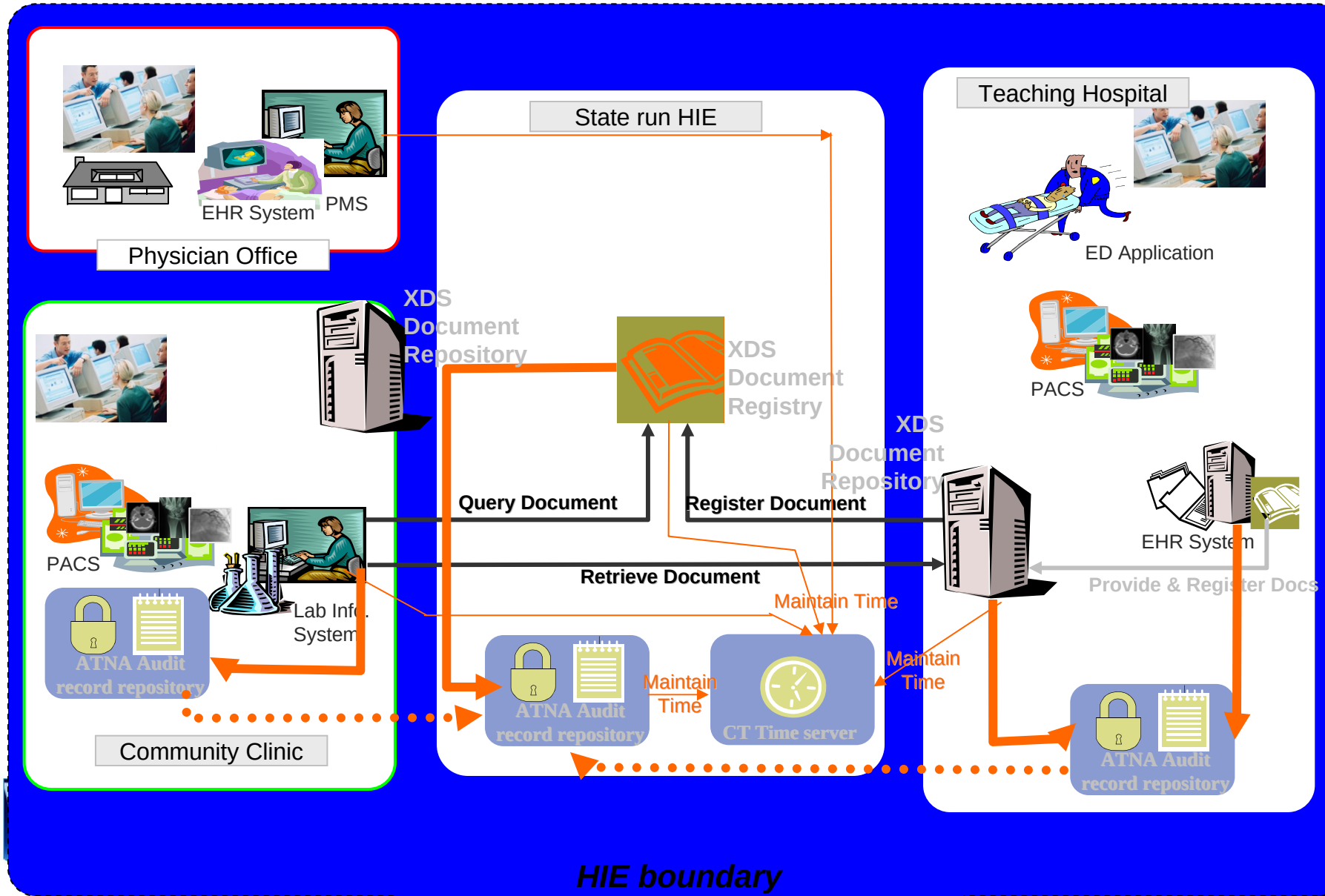
T 15 Collect and Communicate Security Audit Trail



Today's HITSP Accountability

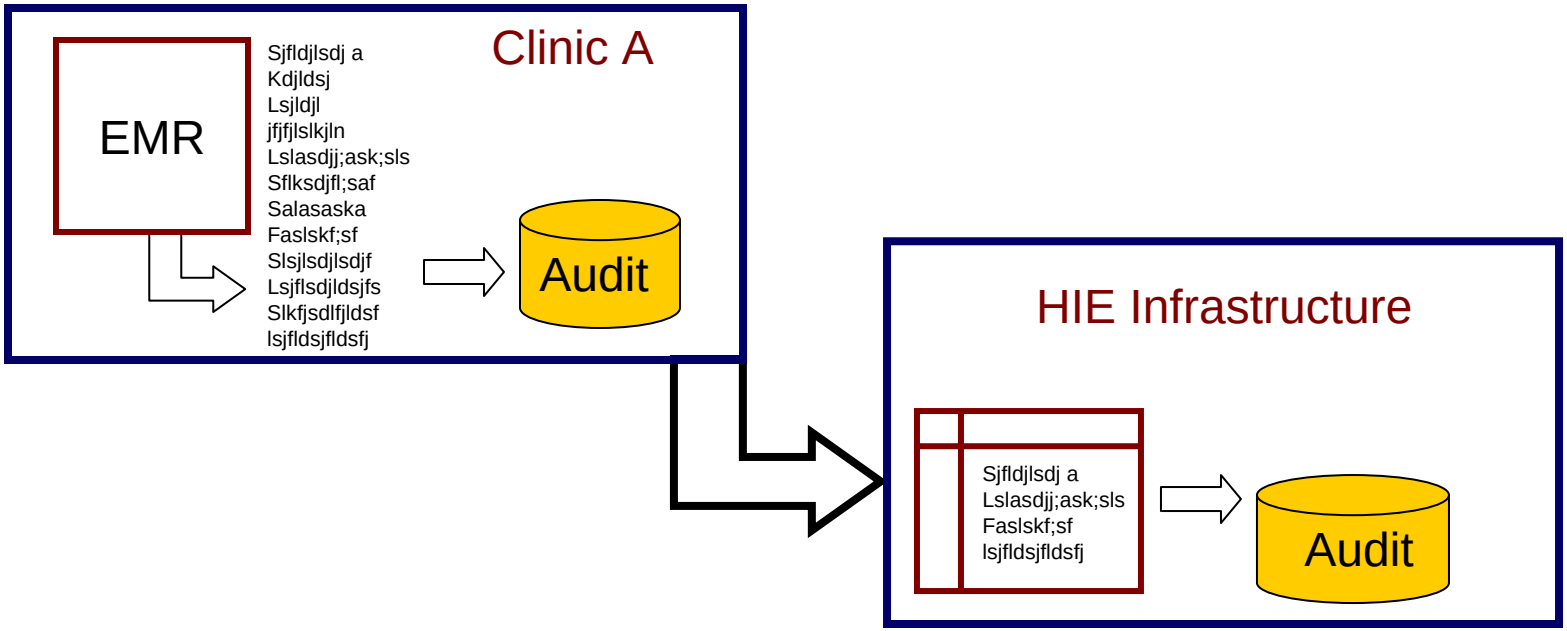
- Investigation of patient complaints
  - Investigate audit log for specific evidence
  - T15 (ATNA) audit repositories can filter and auto-forward
- Support an accounting of disclosures
  - T15 (ATNA Report): XDS-Export + XDS-Import

Distributed Accountability



Example

Audit Log Cascade



- Inform Disclosure Reports
- Detect unusual behavior → Follow chain back

HITSP SPI Constructs

Used across HITSP IS

SPI Constructs	IS01	IS02	IS03	IS04	IS05	IS06	IS07	ISXX
Privacy Controls								
Manage Consent Directives (TP30)	✓	✓	✓	✓	✓	✓	✓	✓
Security Controls								
Collect/Communicate Audit Trail (T15)	✓	✓	✓	✓	✓	✓	✓	✓
Consistent Time (T16)	✓	✓	✓	✓	✓	✓	✓	✓
Secured Communications Channel (T17)	✓	✓	✓	✓		✓	✓	✓
Identity and Access Control								
Entity Identity Assertion (C19)	✓	✓	✓	✓	✓	✓	✓	✓
Access Control (TP20)	✓		✓	✓	✓	✓	✓	✓

ISXX = Initial Assessment of Applicability of SPI Constructs to New 2008 Use Cases

C 19 Entity Identity Assertion

- Value Proposition
  - Extend user identity to web services used
    - Users include Providers, Patients, Clerical, etc
    - Must supports cross-enterprise transactions, can be used inside enterprise
    - Distributed or centralized identity management (directories)
  - Provide information necessary so that receiving actors can make access control decisions
    - Authentication mechanism used
    - Attributes about the user (roles)
    - Does not include access control mechanism
  - Provide information necessary so that receiving actors can produce detailed and accurate security audit trail

C19 Entity Identity Assertion (continued)

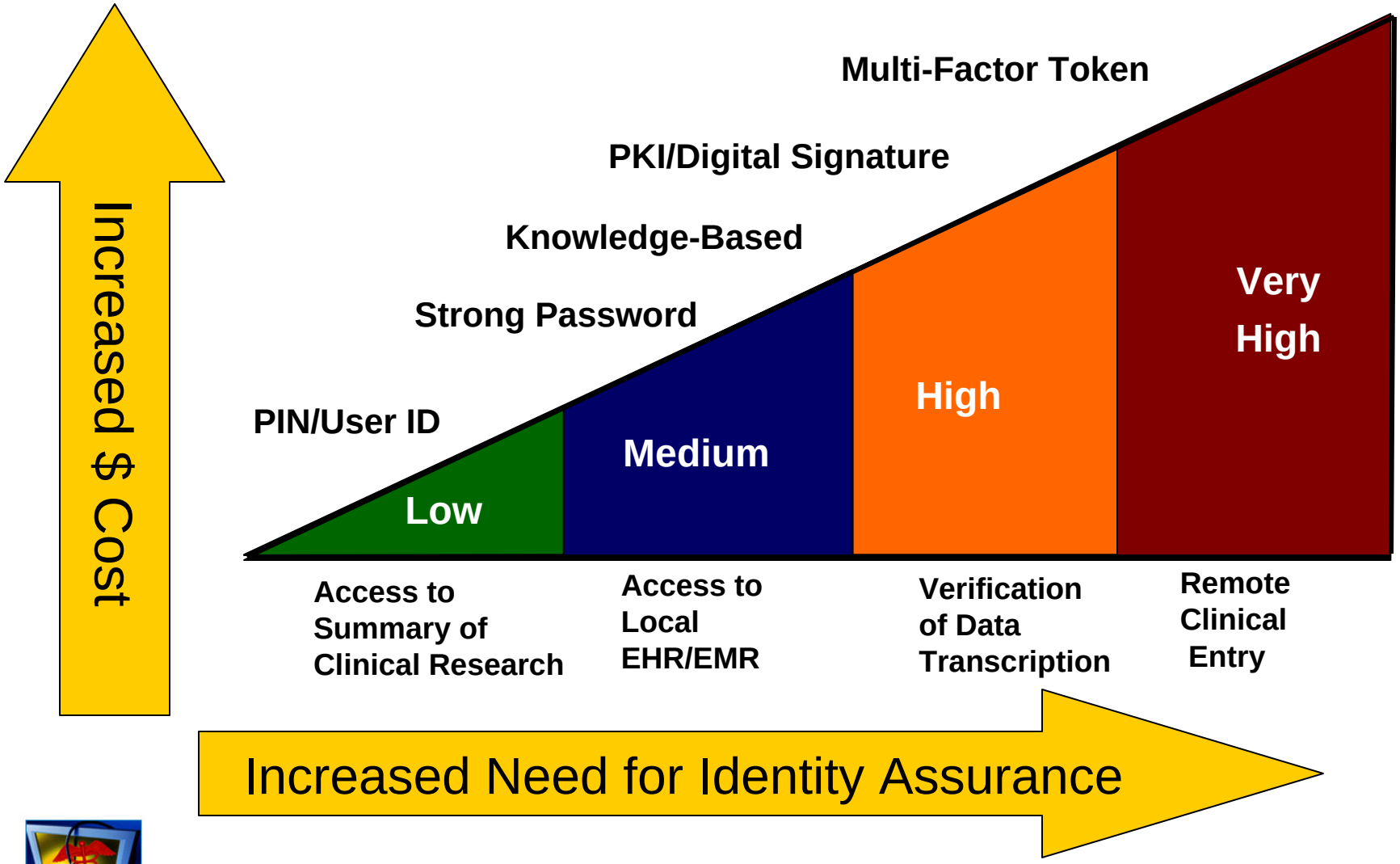
- Concept
  - To ensure that an entity is the person or application that claims the identity provided for access to EHR data in an HIE
  - Example: the validation and assertion of a consumer logging on to a Personal Health Record system

TP 20 Access Control

- Concept
  - to administer security authorizations which control the enforcement of security policies including: role-based access control; entity-based access control; context-based access control; and the execution of consent directives
  - In emergency: construct must support capability to alter access privileges to the appropriate level (failsafe/emergency access), which may include override of non-emergency consents.

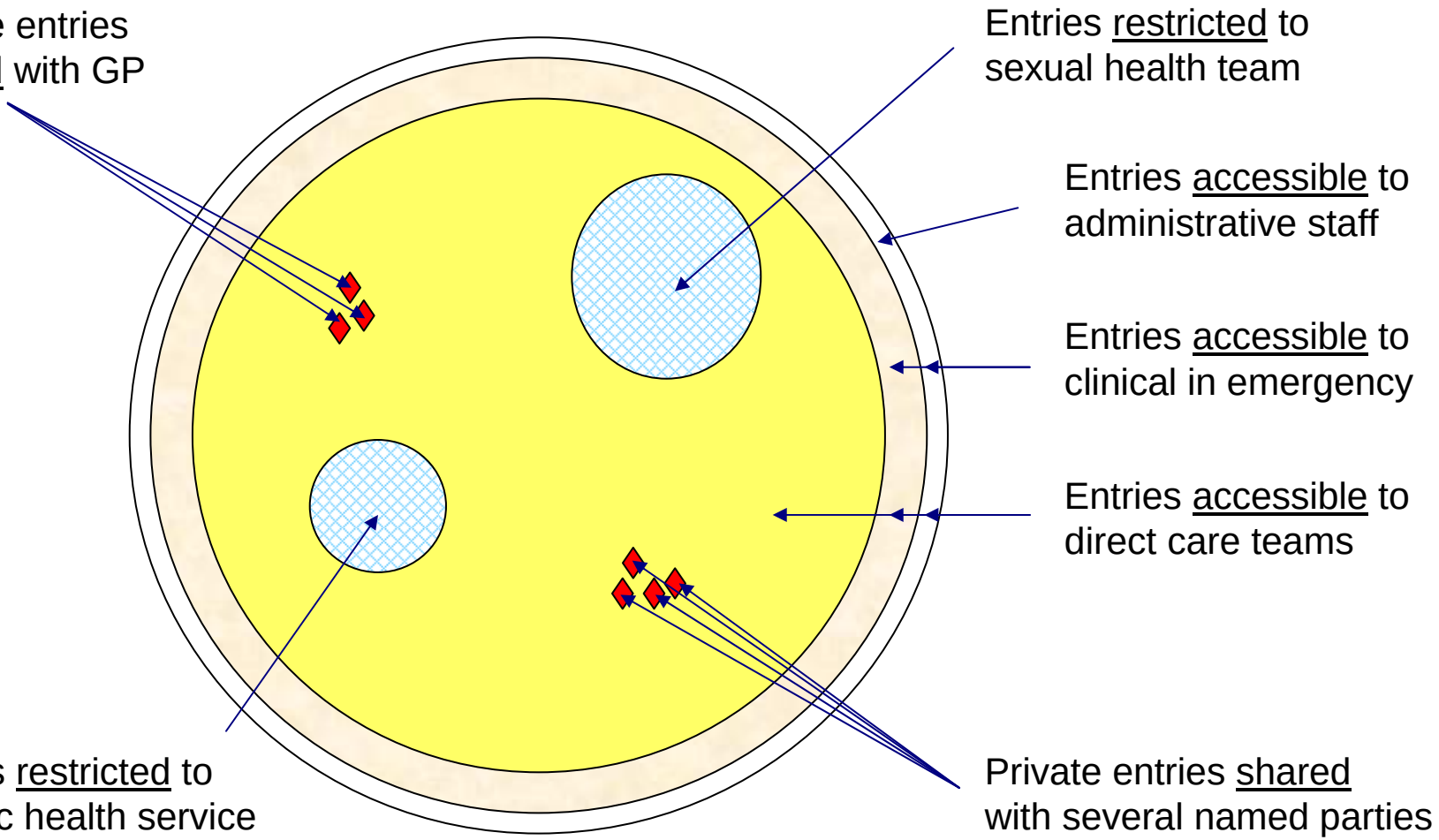
Security Considerations

Four Identity Assurance Levels



Example

Document Accessibility

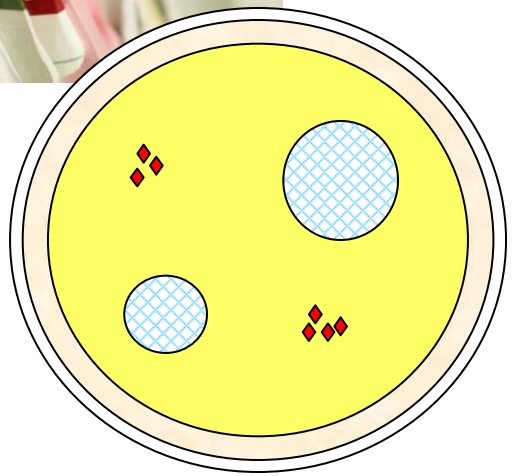


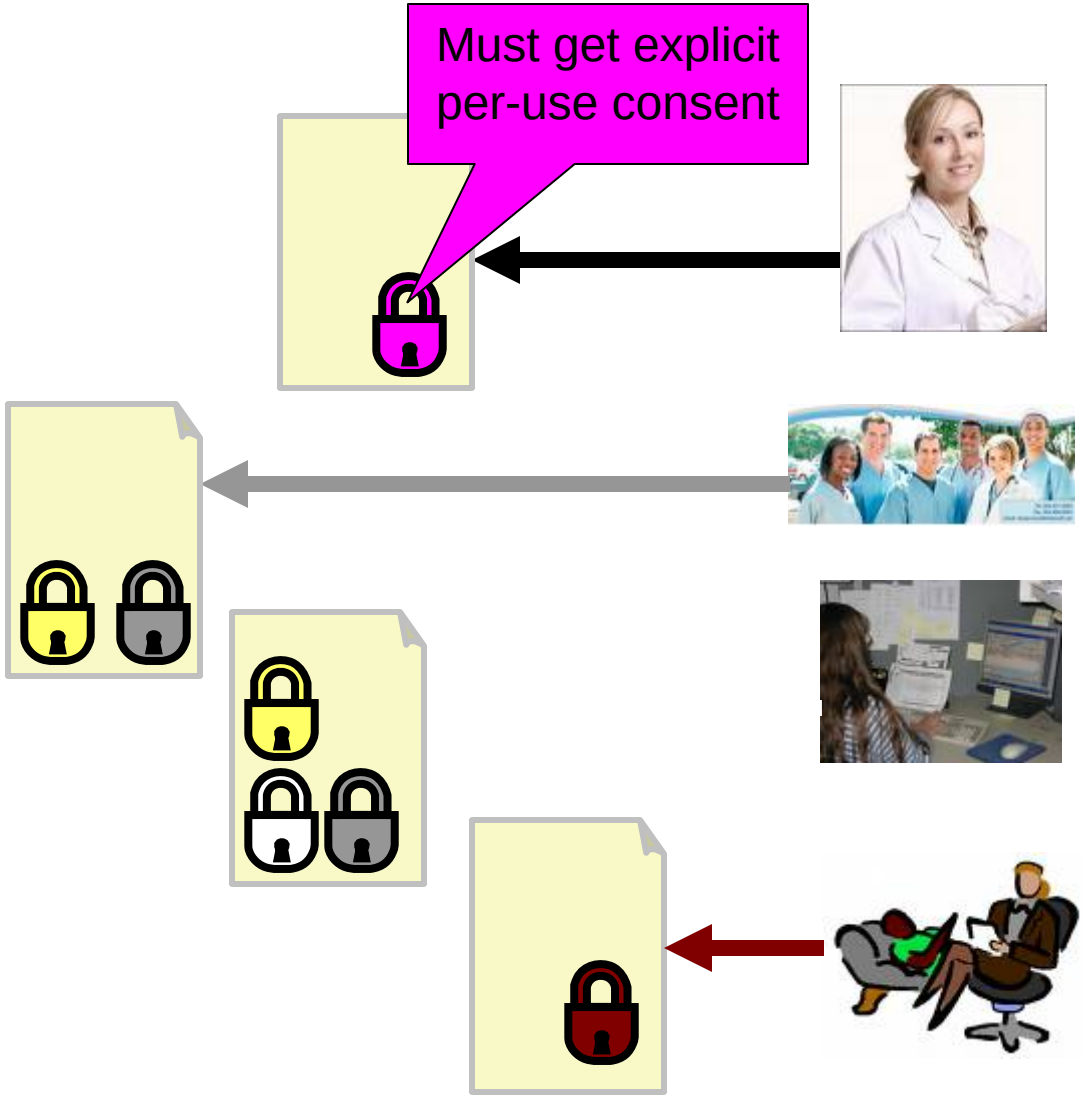
Source: Dipak Kalra & prEN 13606-4

Sample Role-Based Access Control table

Sensitivity Functional Role	Billing Information	Administrative Information	Dietary Restrictions	General Clinical Information	Sensitive Clinical Information	Research Information	Mediated by Direct Care Provider
Administrative Staff	X	X					
Dietary Staff		X	X				
General Care Provider		X	X	X			
Direct Care Provider		X	X	X	X		X
Emergency Care Provider		X	X	X	X		X
Researcher						X	
Patient or Legal Representative	X	X	X	X	X		

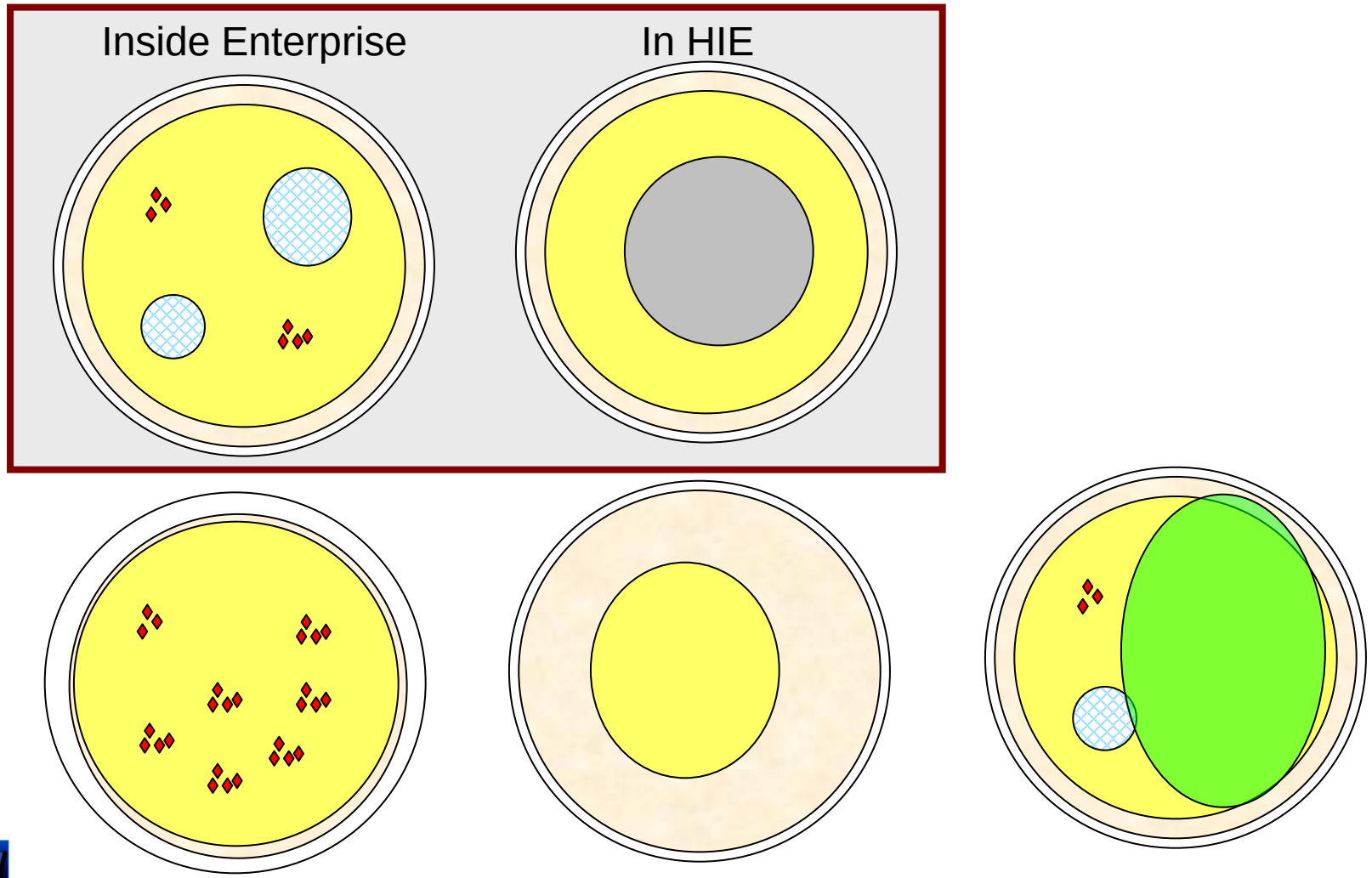
Document Level Controls: ‘confidentialityCode’





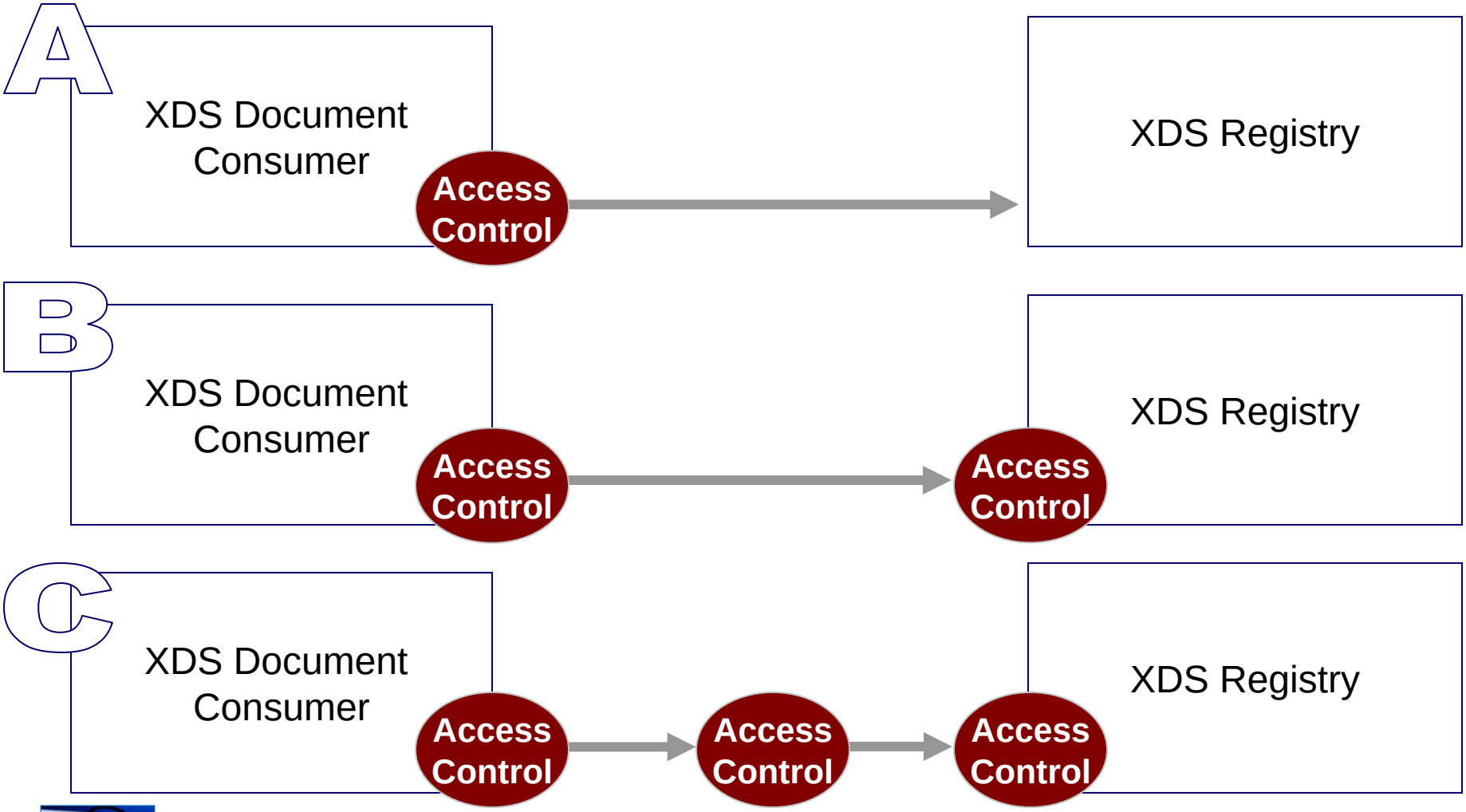
Document Accessibility

There is no single solution



Distributed Access Control

Enabled by C19 – Informed by TP30 - Enforced by TP20



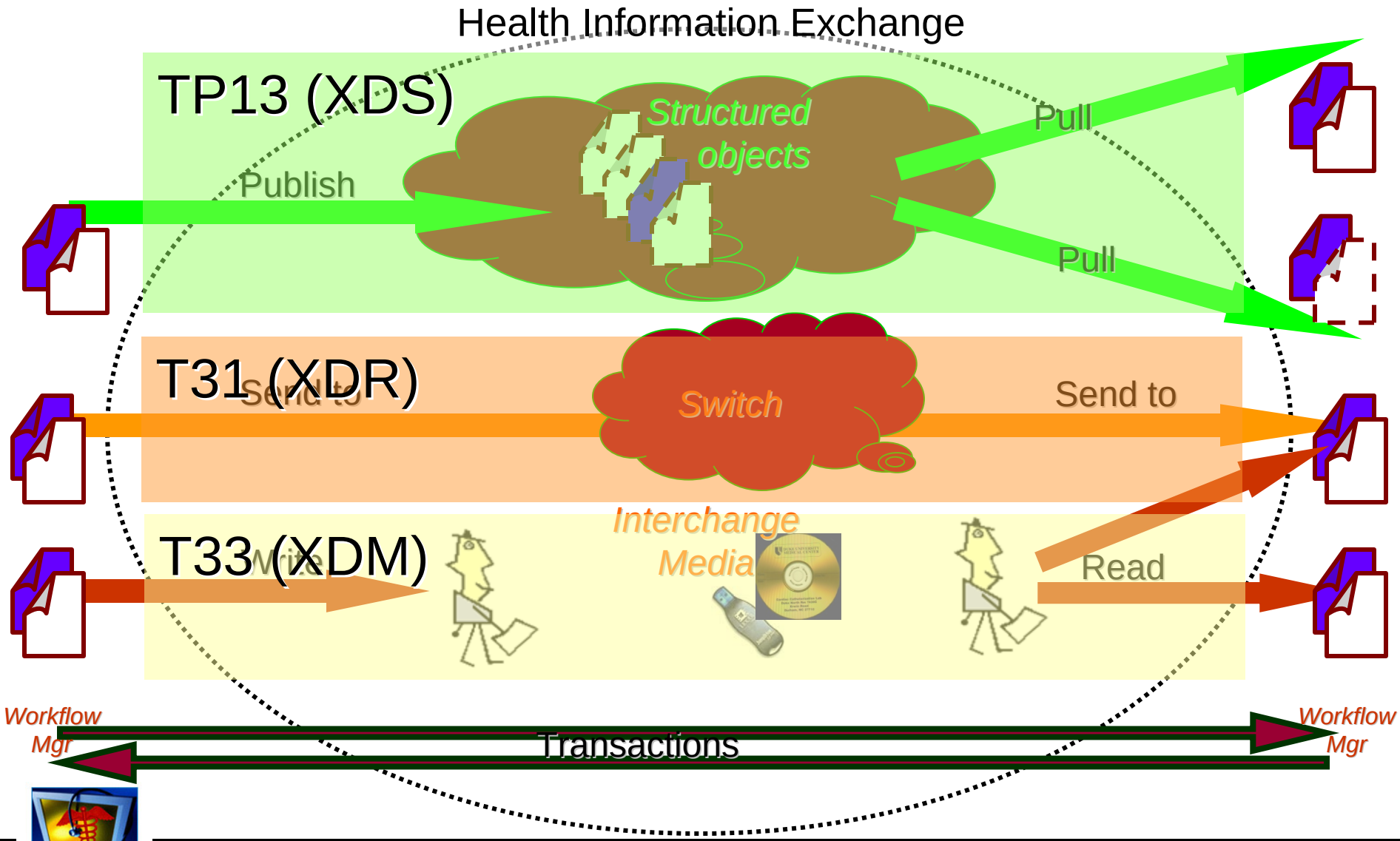
HITSP

Healthcare Information Technology Standards Panel

The bigger picture

Flexible Infrastructure

Sharing, Sending and Interchanging



HITSP Constructs
Mapped to Security/Privacy Controls

Security & Privacy Controls HITSP Construct	Accountability	Identification and Authentication	Data Access	Confidentiality	Data Integrity	Non-Repudiation	Patient Privacy	Availability
TP 13 Manage Sharing of Documents				D	D		I	D
TP 20 Access Controls	D	D	D	D	D	D	D	
TP 30 Manage Consent Directives				I			D	
T 15 Collect and Communicate Security Audit Trail	D	I	I	I	I	D	D	
T 16 Consistent Time	D	I				D		
T 31 Reliable Document Interchange				D	D		I	D
T 33 Document Interchange on Media			I	D	D		I	D
C 19 Entity Identity Assertion	I	D	I	I		I	I	
C 26 High Assurance Nonrepudiation of Origin	D	D			D	D		

D = Direct Relationship **I** = Indirect Relationship

Summary

Security Constructs

HITSP Construct	Standards
TN900 Security and Privacy	n/a
T16 Consistent Time	• IHE CT - Consistent Time
C19 Entity Identity Assertion	• IHE XUA - Cross-Enterprise User Assertion
T15 Collect and Communicate Security Audit Trail	• IHE ATNA - Audit Trail and Node Authentication
	Continued next page

Summary

Security Constructs (continued)

HITSP Construct	Standards
TP 20 Access Control	• IHE ATNA - Audit Trail and Node Authentication • HL7 v3.0 RBAC - RBAC Healthcare Permissions Catalog • OASIS SAML v2.0 - Security Assertion Markup Language • OASIS WS-Trust - Web Services Trust • OASIS WS-Federation - Web Services Federation Language • OASIS XACML - eXtensible Access Control Markup Language
T 17 Secured Communication Channel	• IHE ATNA - Audit Trail and Node Authentication
C 26 Nonrepudiation of Origin	• IHE DSG - Document Digital Signature Content Profile

Summary

Privacy Constructs

HITSP Construct	Standards
TN900 Security and Privacy	n/a
TP30 Manage Consent Directives	• IHE XDS.a, IHE XDS.b - Cross Enterprise Document Sharing • IHE XCA – Cross Community Access • IHE BPPC – Basic Patient Privacy Consents • HL7 v3.0 Privacy Consent • HL7 Confidentiality Codes • HL7 v3.0 RBAC – Healthcare Permissions Catalog

Summary

Infrastructure Constructs

HITSP Construct	Standards
TP 13 Manage Sharing of Documents	• IHE XDS.a, IHE XDS.b - Cross Enterprise Document Sharing • IHE XCA – Cross Community Access
TP 21 Query for Existing Data	• IHE QED - Query for Existing Data
TP 22 Patient ID Cross-Referencing	• IHE PIX - Patient ID Cross-Referencing
T 23 Patient Demographics Query	• IHE PDQ - Patient Demographics Query
TP 50 Retrieve Form for Data Capture	• IHE RFD - Retrieve Form for Data Capture
T 29 Notification of Document Availability	• IHE NAV – Notification of Document Availability
T 31 Document Reliable Interchange	• IHE XDR – Cross-Enterprise Document Reliable Interchange
T 33 Transfer of Documents on Media	• IHE XDM – Cross-Enterprise Document Media Interchange

Conclusion

- HITSP provides the necessary basic security today
- There is room for improvement – and YOU can help
- Roadmap includes prioritized list of use cases
- Continuous risk assessment is necessary at all levels
  - Product design
  - Implementation
  - Organizational
  - HIE domain

HITSP
Healthcare Information Technology Standards Panel

How YOU can become involved

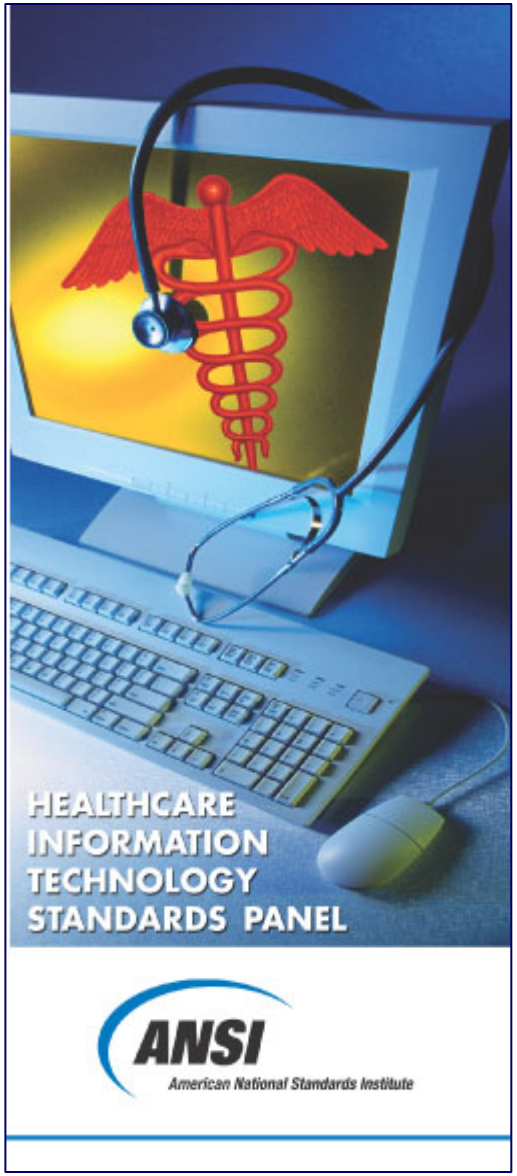
- Use or specify HITSP Interoperability Specifications in your HIT efforts and in your Requests for Proposals (RFPs)
- Ask for CCHIT certification
- Leverage Health Information Exchanges to promote HITSP specifications to make connections easier in the future
- Ask . . . Is there a HITSP standard we could be using?
- Get involved in HITSP . . . Help shape the standards

HITSP
Healthcare Information Technology Standards Panel

How YOU can become involved

Learn more about specific HITSP activities during these upcoming webinars:

Webinar 1 Standardizing How We Share Information in Healthcare: An Introduction to HITSP Thursday, June 5, 2008 — 2:00-3:30 pm EDT ☑	**Webinar 6** Quality **New date** Thursday, October 2, 2008 — 2:00-3:30 pm EDT
Webinar 2 HITSP Foundational Components Thursday, June 19, 2008 — 2:00-3:30 pm EDT ☑	**Webinar 7** Security, Privacy and Infrastructure Thursday, August 21, 2008 — 2:00-3:30 pm EDT ☑
Webinar 3 Consumer Access to Clinical Information Thursday, June 26, 2008 — 2:00-3:30 pm EDT ☑	**Webinar 8** EHR and Emergency Response Thursday, September 4, 2008 — 2:00-3:30 pm EDT
Webinar 4 Biosurveillance Thursday, July 10, 2008 — 2:00-3:30 pm EDT ☑	**Webinar 9** Medication Management Thursday, September 18, 2008 — 2:00-3:30 pm EDT
Webinar 5 Electronic Health Record (EHR) and Lab Reporting Thursday, July 24, 2008 — 2:00-3:30 pm EDT ☑	**www.HITSP.org/webinars**



Join HITSP in developing a safe and secure health information network for the United States.

Visit **www.hitsp.org** or contact . . .

Michelle Deane, ANSI
mmaasdeane@ansi.org

Re: HITSP, its Board and Coordinating Committees

Jessica Kant, HIMSS
jkant@himss.org

Theresa Wisdom, HIMSS
twisdom@himss.org

Re: HITSP Technical Committees

HITSP

Healthcare Information Technology Standards Panel

Sponsor

ANSI
American National Standards Institute

Strategic Partners

ATI
Advancing Technology through Collaboration

Booz | Allen | Hamilton

HIMSS
transforming healthcare through IT

www.HITSP.org

Webinar Series

HITSP

Healthcare Information Technology Standards Panel

Security, Privacy and Infrastructure (SPI)

Privacy is the goal – Security is the way

Sponsored by the HITSP Education, Communications and Outreach Committee