



Managing Consent Directives

Electronic Standards to Capture, Report and Implement Health Information Privacy Consent

August 27, 2008 | 2:00 – 3:30 pm (Eastern)

Presenters:

John Moehrke – GE Healthcare; Co-Chair, HITSP Security, Privacy and Infrastructure Technical Committee

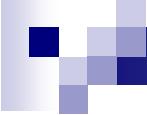
Walter G. Suarez, MD – Institute for HIPAA/HIT Education and Research; Co-Chair, HITSP Security, Privacy and Infrastructure Technical Committee

Moderator:

Johnathan Coleman – Security Risk Solutions, Inc.; Lead Facilitator, HITSP Security, Privacy and Infrastructure Technical Committee

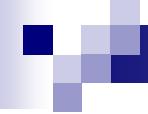
* Please note all participants were placed on mute as they joined the webinar.

Funded by the Agency for Healthcare Research and Quality



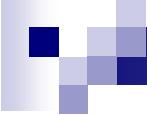
Outline

- **Welcome** — Johnathan Coleman
- **Before We Begin** — Johnathan Coleman
- **Introductions** — Johnathan Coleman
- **Presentations**
 - Walter Suarez
 - John Moehrke
- **Question and Answer** — Johnathan Coleman
- **Closing Remarks** — Johnathan Coleman



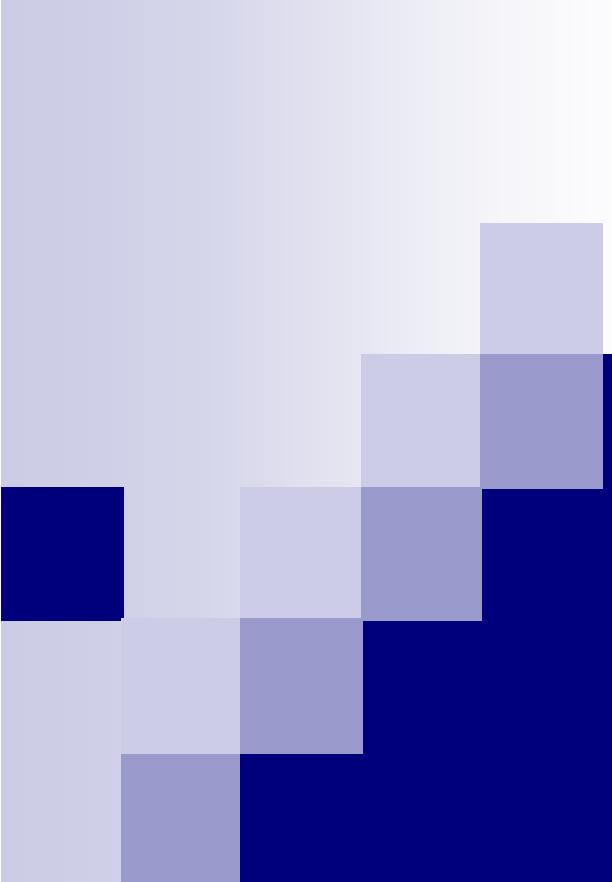
Before we begin...

- Please note all participants were muted as they joined the Webinar.
- If you have a question during the presentation, please send your question to ***all panelists*** through the chat. At the end of the presentation, there will be a question and answer period.
- If at any time you wish to be unmuted to post a question “live”, please choose the “raise hand” option on the Webinar console to notify the host.
- Webinar is being recorded. The AHRQ-RTI Team will post all TA presentation materials, the audio portion of the Webinar and a transcript to the project website shortly after the completion of the Webinar - <http://healthit.ahrq.gov/Medicaid-SCHIP>.
- You may also e-mail Nicole Buchholz at nbuchholz@rti.org if you would like a copy of today’s presentation slides.

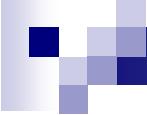


Project Listserv Registration

- Please register for the listserv to receive announcements about program updates and upcoming TA Webinars.
- To register go to <http://healthit.ahrq.gov/Medicaid-SCHIP>.
- Click on “Medicaid-SCHIP Fast Facts” on the left-hand side of the screen
- There are two ways to register for the listserv:
 - 1. Click the link [Click here to subscribe to the listserv](#), which will open a pre-filled email message, enter your name after the text in the body of the message and send.
 - 2. Send an e-mail message to: listserv@list.ahrq.gov. On the subject line, type: **Subscribe**. In the body of the message type: **sub Medicaid-SCHIP-HIT** and **your full name**. For example: sub Medicaid-SCHIP-HIT John Doe. You will receive a message asking you to confirm your intent to sign up.

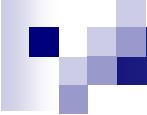


Introduction and Overview



Learning Objectives

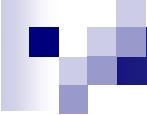
- Review core privacy concepts applicable to the development of interoperable standards for patient privacy consent directives
- Introduce/review the HITSP Manage Consent Directives construct that establishes the national harmonized interoperable standards to be used when capturing, maintaining, reporting and implementing privacy consent directives given by a patient or consumer
- Review examples of how the new consent standards can be used in the marketplace
- Discuss the applicability of the construct to Medicaid/SCHIP programs



Basic Concepts

- What is Privacy (of health information)?
 - An individual's (or organization's) right to determine whether, what, when, by whom and for what purpose their personal health information is collected, accessed, used or 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

Source: HITSP Vocabulary – modified and expanded from 45 CFR 164.304



Basic Concepts

- **Confidentiality**

- The property that data or information is not made available or disclosed to unauthorized persons or processes

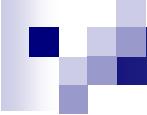
- **Integrity**

- 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

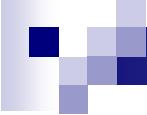
Source: 45 CFR 164.304



Privacy of Health Information

– Important Underlying Realities

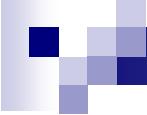
- Medical records among the most sensitive information about a person
- Health care is an information-driven field
 - Everything about the health care system involves information
 - Information is much more complex than other industries (amount, type, frequency)
- Health information is central to the doctor-patient relationship
- Privacy and security of health information are central to the doctor-patient relationship



Privacy of Health Information

– *Important Underlying Realities*

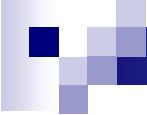
- Health care is a complex system when it comes to health information
 - Many actors (patient, provider, health plan, employer, government, public health, researchers, vendor, etc.)
 - Various types of information (demographic, clinical, financial)
 - Many processes related to health information (collection, creation, maintenance, access, use, disclosure)
 - Different purposes (treatment, payment, operations, public health, research, judicial, legal, etc.)
 - Many places where health information resides
 - Lack of common identifiers and other standards



Privacy of Health Information

– *Important Underlying Realities*

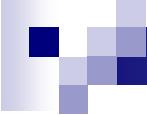
- Many laws
 - Federal laws, including HIPAA, Privacy Act, Education Records Law, Mental health records laws, Public health information laws
 - State laws are a patchwork of varying types and levels of state privacy laws, few addressing health privacy and security in a comprehensive fashion
- Different policies and practices created and used by organizations
 - Many go above and beyond what federal/state laws require



Privacy of Health Information

– *Important Underlying Realities*

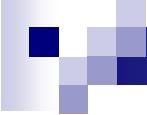
- Increasing complexities
 - Expanded use of electronic health records
 - Increased electronic communications between patients and the health care system (i.e., websites, e-mail)
 - Electronic networks (Regional Health Information Exchanges, NHIN)
 - Evolving personal health records



Privacy of Health Information

– *Current Practices*

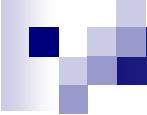
- HIPAA has generally defined the floor for uses and disclosures of health information
- HIPAA did not require “consent” for uses or disclosures related to treatment, payment and health care operations
 - “Authorization” required for other specific uses and disclosures
- HIPAA does not define requirements for
 - Electronic consent
 - Granularity of consumer controls
 - Electronic health information exchanges
 - Personal health records



Privacy of Health Information

– *Current Practices*

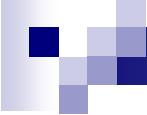
- Other Federal laws define specific use and disclosure requirements (over and above HIPAA) for specific types of data (i.e., substance abuse, mental health, lab data, education records)
- There are also program-specific privacy protection requirements (such as Medicare, Medicaid, SCHIP)
- Many state laws establish additional requirements for when privacy consent is needed
 - Some require consent even for treatment, payment and operations
 - Still most are silent about electronic consent, granularity, electronic health information exchanges, personal health records



Privacy of Health Information

– *Current Practices*

- Most consumer privacy conducted via paper forms
 - General consumer privacy consent offered at initial point of care/enrollment (when required)
 - Additional patient consent/authorization for specific health information, specific disclosure purposes (when required)
 - No standard paper consent forms within a jurisdiction (state)
 - Each organization/program has its own forms
 - Some States are beginning to establish a standard form
- Most current requirements focus on uses and disclosures (including access)
 - Very little on collection of health information

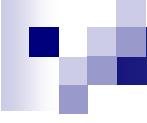


Privacy of Health Information

– *Portability Issues*

■ Inter-jurisdictional Portability

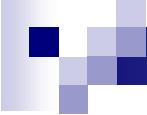
- Consumer privacy consent laws and requirements, and consumer privacy desires and directives in one jurisdiction may not be legally applicable/enforceable in another jurisdiction
 - An entity operating in one jurisdiction uses and discloses health information based on its own policies and procedures, created to meet consent requirements under that jurisdiction
 - When information is disclosed to a different entity in another jurisdiction, the receiving entity applies its own policies and procedures to the received data, which were created to meet consent requirements under the receiving entity's jurisdiction



Privacy of Health Information

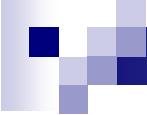
– *Cross-validation Issue*

- Cross-validation and verification of conflicting consents
 - What is the most recent/latest consent from a patient?
 - Does that override other consents for specific data, specific purpose?
 - Where can I find the various consents issued by a consumer to perform cross-validation and verification?



Electronic Standards for Consumer Consent – A New Paradigm

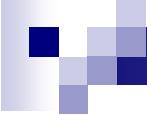
Offer consumers and the health care industry an interoperable, standards-based electronic mechanism to collect, capture, maintain, report, transfer and act upon consumer consent directives, in a manner that allow users to meet different types of jurisdictional requirements



Electronic Standards for Consumer Consent

– *What are Privacy Consent Directives?*

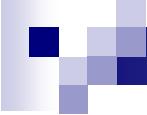
- A Consent Directive is a record of a consumer's privacy policy, in accordance with governing jurisdictional and organization privacy policies, that grant or withhold consent:
 - To one or more identified entities in a defined role
 - To perform one or more operations (e.g., collect, access, use, disclose, amend, or delete)
 - On an instance or type of health information
 - For a general or specific purpose, such as treatment, payment, operations, research, public health, quality measures, health status evaluation by third parties, or marketing
 - Under certain conditions (e.g., when unconscious)
 - For specified time period (e.g., effective and expiration dates)
 - In certain contexts (e.g., in an emergency)



Electronic Standards for Consumer Consent

– *Key Characteristics*

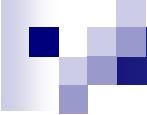
- Consumer-friendly mechanism
 - To allow consumers to manage their consent directives electronically in a simple, reliable, secure, efficient and effective manner
- Scalable
 - Allow to go from General (overall opt-in/opt-out) to Granular (specific data, specific people, specific people)
- Codifiable
 - Uses standard codes to express consent directives



Electronic Standards for Consumer Consent

– *Key Characteristics*

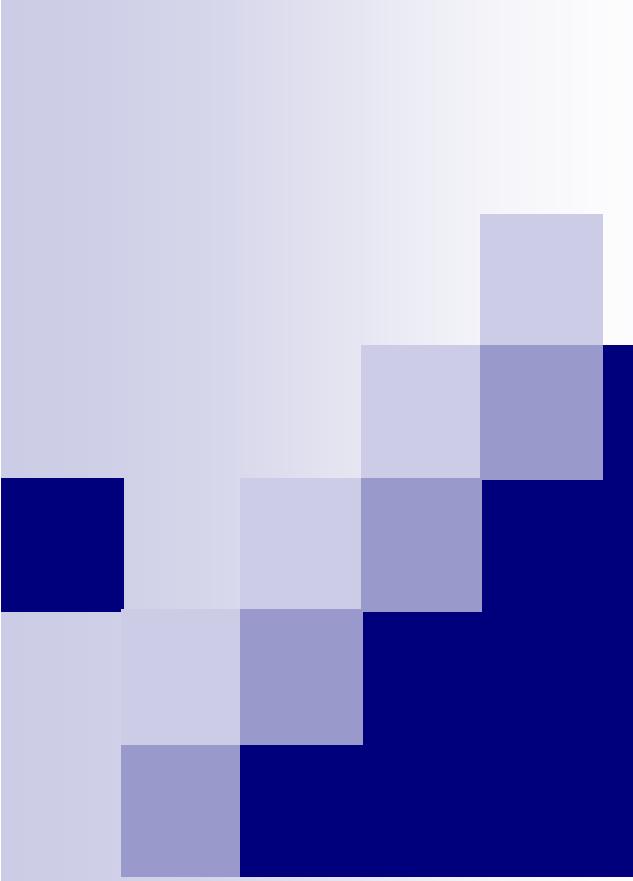
- Machine-readable/Machine-actionable
 - Does not require human intervention to process
 - Allow systems to operationalize, access, use and disclosure controls
- Portable/Transferable
 - Can be electronically ported/transferred between organizations and across jurisdictions



Electronic Standards for Consumer Consent

– *Key Characteristics*

- **Flexible/Adaptable**
 - Features can be “turned-on” or “turned-off” based on differing levels of jurisdictional requirements
- **Valid/Verifiable/Auditable**
 - Supports digital signature, non-repudiation, audit controls
- **Unambiguous/Completeness**
 - Conflicts between directives can be identified and resolved



The HITSP Standards for Consent Directives



Who is HITSP?

- Volunteer-driven, consensus-based organization that is funded through a contract from the Department of Health and Human Services
- The Panel brings together experts from across the healthcare community
 - from ***consumers to doctors, nurses, and hospitals***
 - from ***those who develop*** healthcare IT products to ***those who use them***
 - from the ***government agencies*** who monitor the U.S. healthcare system to those ***organizations that are actually writing healthcare IT standards***



Healthcare Information Technology Standards Panel

Roles and Responsibilities

- To harmonize and recommend the technical standards that are necessary to ensure the interoperability of electronic health records
 - Create HITSP-recommended Interoperability Specifications (IS) that specify how and what standards should be used for a particular Use Case
 - Support deployment and implementation of these HITSP-recommended Interoperability Specifications
 - Help Standards Development Organizations (SDOs) maintain, revise or develop new standards as required to support the HITSP-recommended Interoperability Specifications



Healthcare Information Technology Standards Panel

Deliverables and Mode of Operation

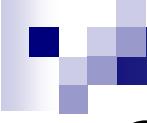
- Identify a pool of standards for an AHIC Use Case
- Identify gaps and overlaps in the standards for this specific Use Case
- Make recommendations for resolution of gaps and overlaps
- Select standards using HITSP Approved Readiness Criteria
- Develop Interoperability Specifications (IS) for using the selected standard(s) for the specific context
- Test the IS

Security, Privacy and Infrastructure (SPI) – *Core Components of the HITSP Work*

- HITPS SPI Goal: To identity, evaluate and recommend security, privacy and infrastructure constructs that address interoperability needs and requirements defined by the AHIC-ONC Uses Cases
- Process:
 - Identify Security, Privacy and Infrastructure needs (requirements) from AHIC use-cases
 - Identify Candidate Standards and evaluate/select standards for interoperability, based on HITSP Tier 2 Criteria
 - Identify and document constructs which describe implementation of the selected standards and maximize the potential for re-use in future AHIC Use Cases



HITSP
Healthcare Information Technology Standards Panel



Security, Privacy and Infrastructure (SPI) – *Core Components of the HITSP Work*

- Recommend to AHIC the selected constructs for acceptance and recognition by the Secretary
 - Incorporate the applicable constructs throughout all HITSP **Interoperability Specifications** (ISs)
 - Maintain/update constructs periodically (and develop new ones, as needed) based on new use cases issued by AHIC



HITSP
Healthcare Information Technology Standards Panel

Security, Privacy and Infrastructure (SPI) and Healthcare Information Interoperability

■ **Security**

Elements such as consistent time, secure communications channel, entity identity assertion, and others

■ **Privacy**

Elements related to capturing and reporting consent directives electronically

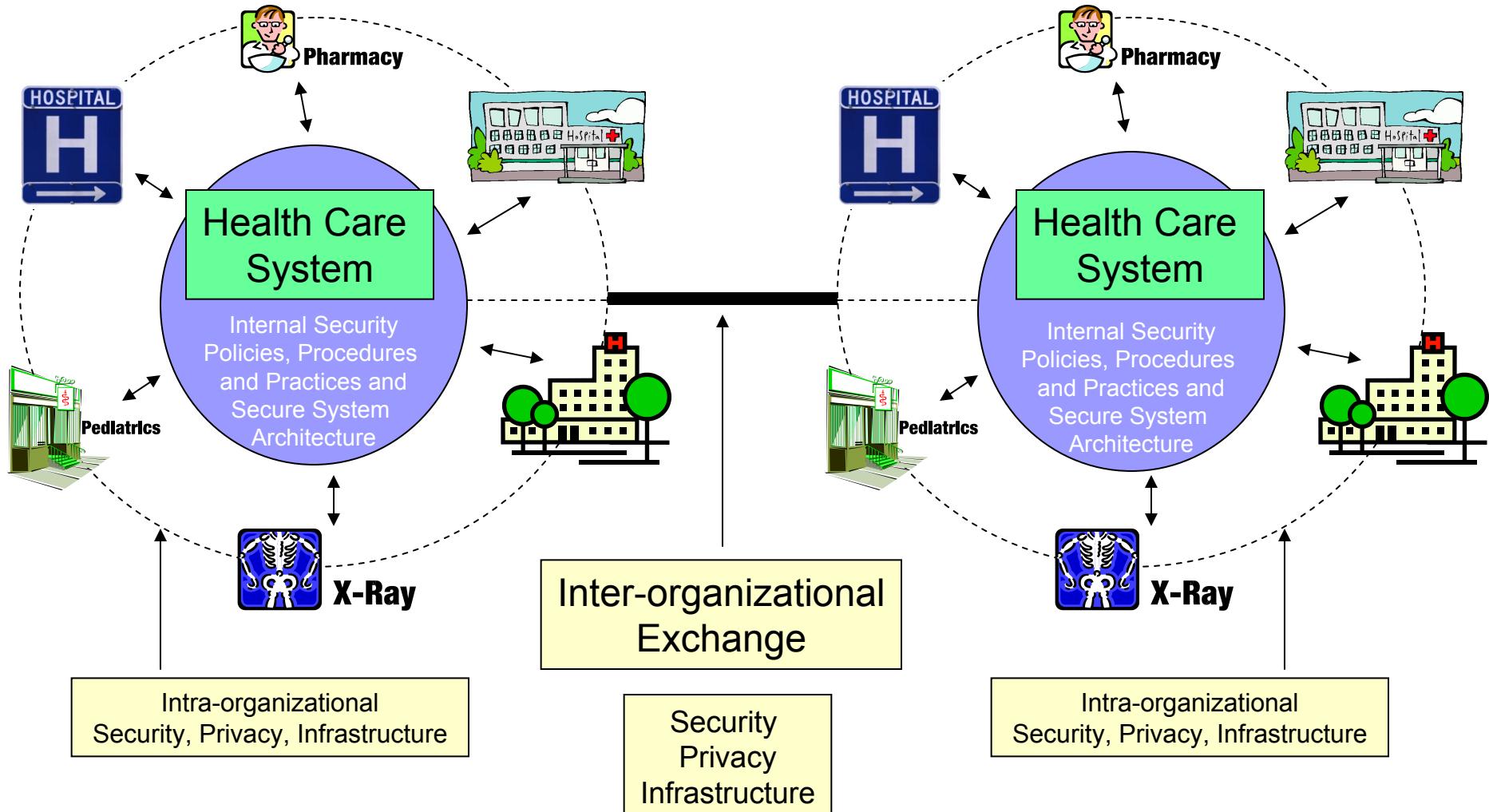
■ **Infrastructure**

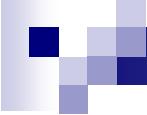
Structural elements of the exchange of health information, such as querying for existing data or notification of document availability



HITSP
Healthcare Information Technology Standards Panel

Interoperability – The Focus of HITSP



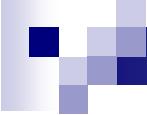


Privacy and Security Scenarios

- 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)
- Caregiver (assists with care)

HITSP SPI Constructs

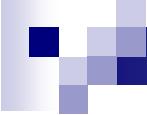
- Provide Entity Identity Assertions
- Manage consumer privacy
Consent Directives (TP30)
- Establish and manage
Access Controls
- Ensure Management of Document Sharing
- Utilize a Secure Communication Channel
- Implement Nonrepudiation of Origin
- Collect/communicate
Security Audit Trails
- Consistent use and control of system Time
- Provide Patient Demographics Query
- Ensure Document Reliable Exchange
- Establish Patient ID Cross-Referencing
- Provide Notification of Document Availability
- Utilize Secure Web Connection
- Allow secure Transfer of Documents on Media
- Support Query for Existing Data
- Support the ability to Retrieve Form for Data Capture
- Provide ability to Pseudonymize and Anonymize data



HITSP TP30 – *Manage Consent Directives*

Value Proposition

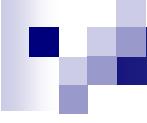
- An HIE can
 - develop privacy policies
 - implement them with role-based or other access control mechanisms supported by edge/EHR systems
- A patient can
 - be made aware of an institution privacy policies
 - have an opportunity to selectively control access to his or her healthcare information



HITSP TP30 – *Manage Consent Directives*

Abstract

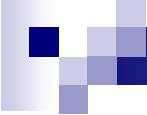
- Concept:
 - Manage Patient Consent choices
- Selected Composite Standards:
 - IHE Basic Patient Privacy Consent (BPPC) Profile
 - IHE XDS (via TP13)
 - Cross-Enterprise Document Sharing (XDS.a, XDS.b, XDR, and XDM)
 - XDS Scanned Documents



HITSP TP30 – *Manage Consent Directives*

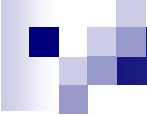
Abstract (cont.)

- Selected Base Standards:
 - HL7 Data Consent Message
 - HL7 Confidentiality Codes
 - HL7 v3.0 Consent Related Vocabulary
- Other Standards
 - CDA Release 2.0
 - Document Digital Signature
- Key Properties
 - Human Readable Consents
 - Machine Processable
 - Support for standards-based Role-Based Access Control



HITSP TP30 – *Manage Consent Directives: Base/Composite Standards*

- **The Basic Patient Privacy Consents (BPPC) profile provides mechanisms to**
 - record the patient privacy consent(s)
 - mark documents published to XDS/XDR/XDM with the patient privacy consent(s) used to authorize the publication
 - enforce the privacy consent(s) appropriate to the use.



HITSP TP30 – *Manage Consent Directives: Base/Composite Standards*

HL7 confidentiality codes

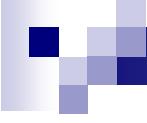
Normative Codes

N Normal

S Sensitive

Other Normative Codes Being Considered

HIE-Defined Codes May Be Supported

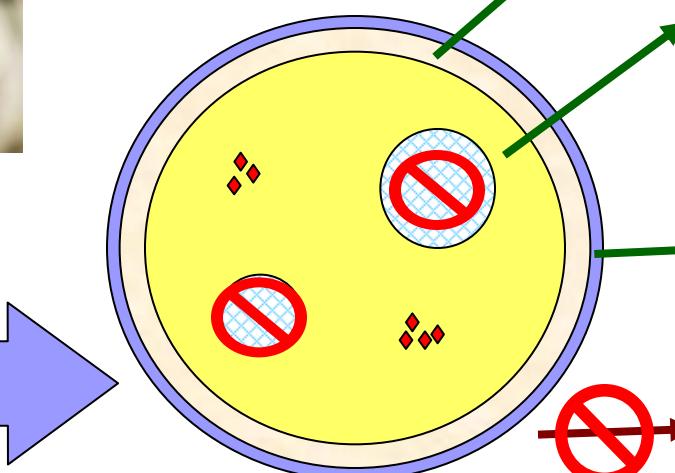


HITSP TP30 – *Manage Consent Directives: Base/Composite Standards*

HL7 Permission codes

PRD-006	Patient Identification and Lookup
PRD-017	Review Progress Notes
PRD-012	Review Past Visits
PRD-003	Review Medical History
PRD-005	Review Vital signs/Patient Measurements
PRD-009	Review Current Directory of Provider Information
PRD-010	Review Patient Medications
...	...

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



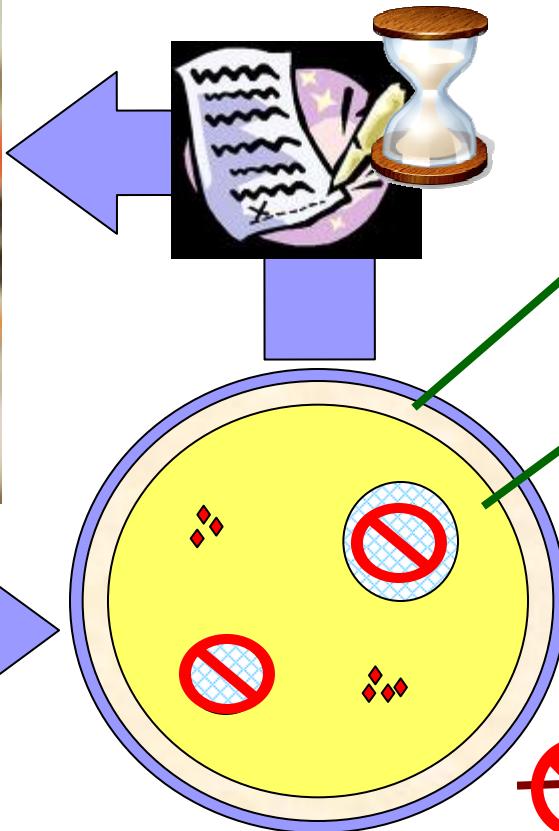
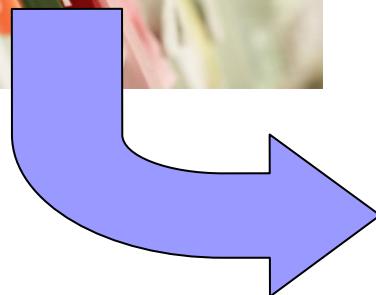
Entries accessible to administrative staff



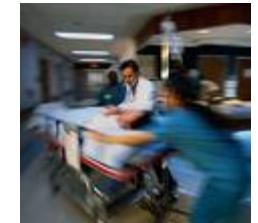
Entries accessible to research staff



Basic Consent on an Episode basis (continued)



Entries accessible to clinical in emergency



Entries accessible to direct care teams



Entries accessible to administrative staff

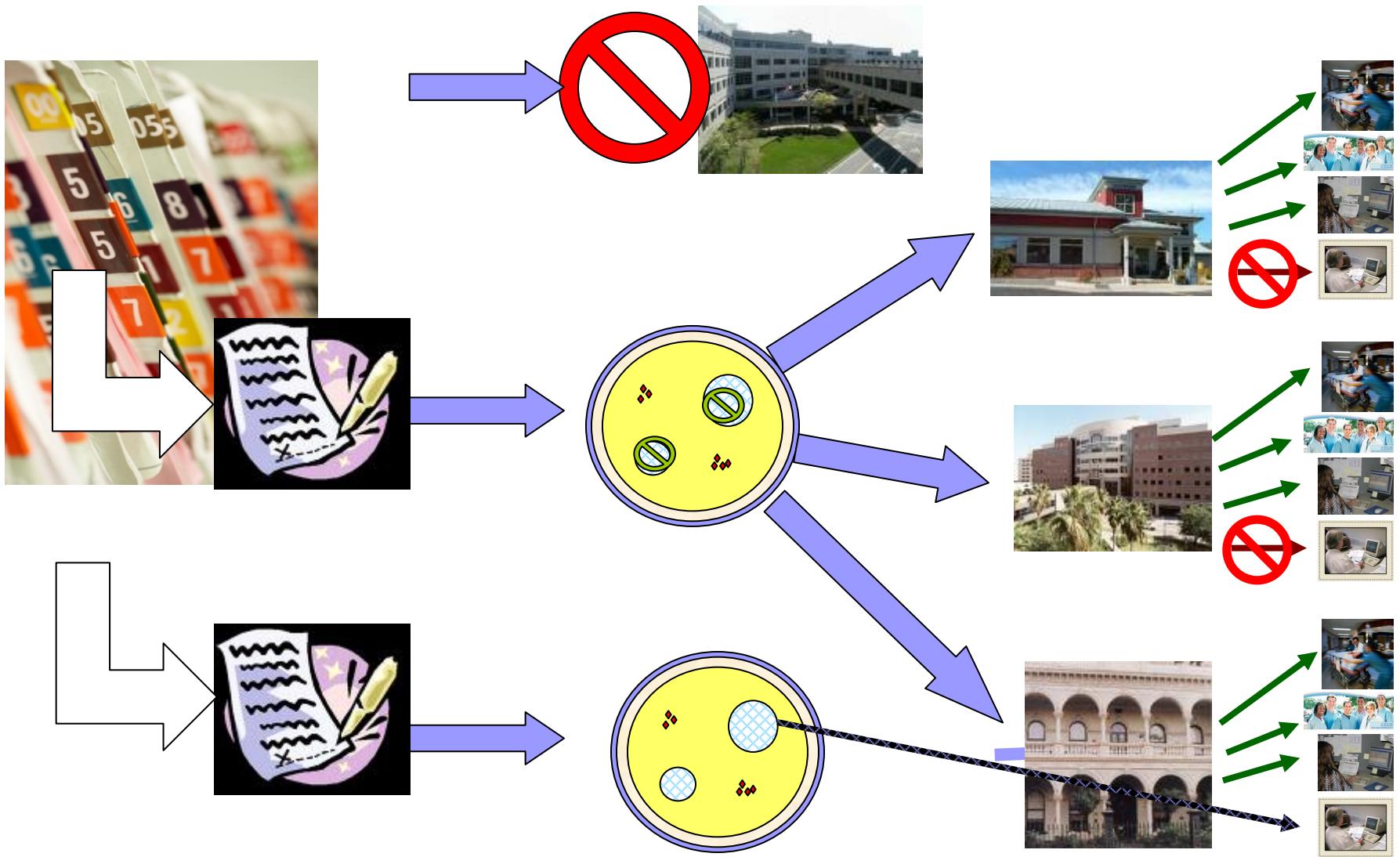


Entries accessible to research staff

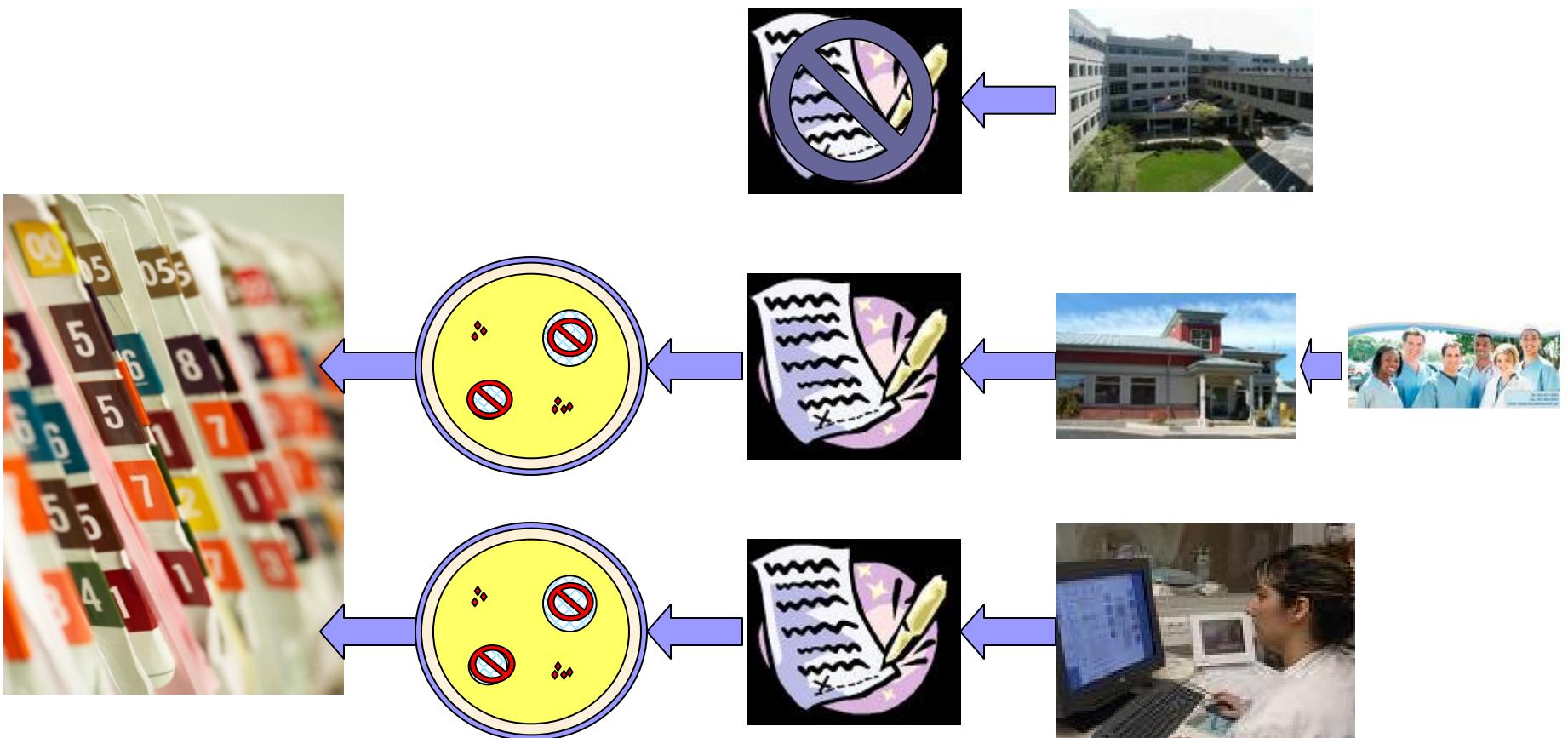


Basic Consent

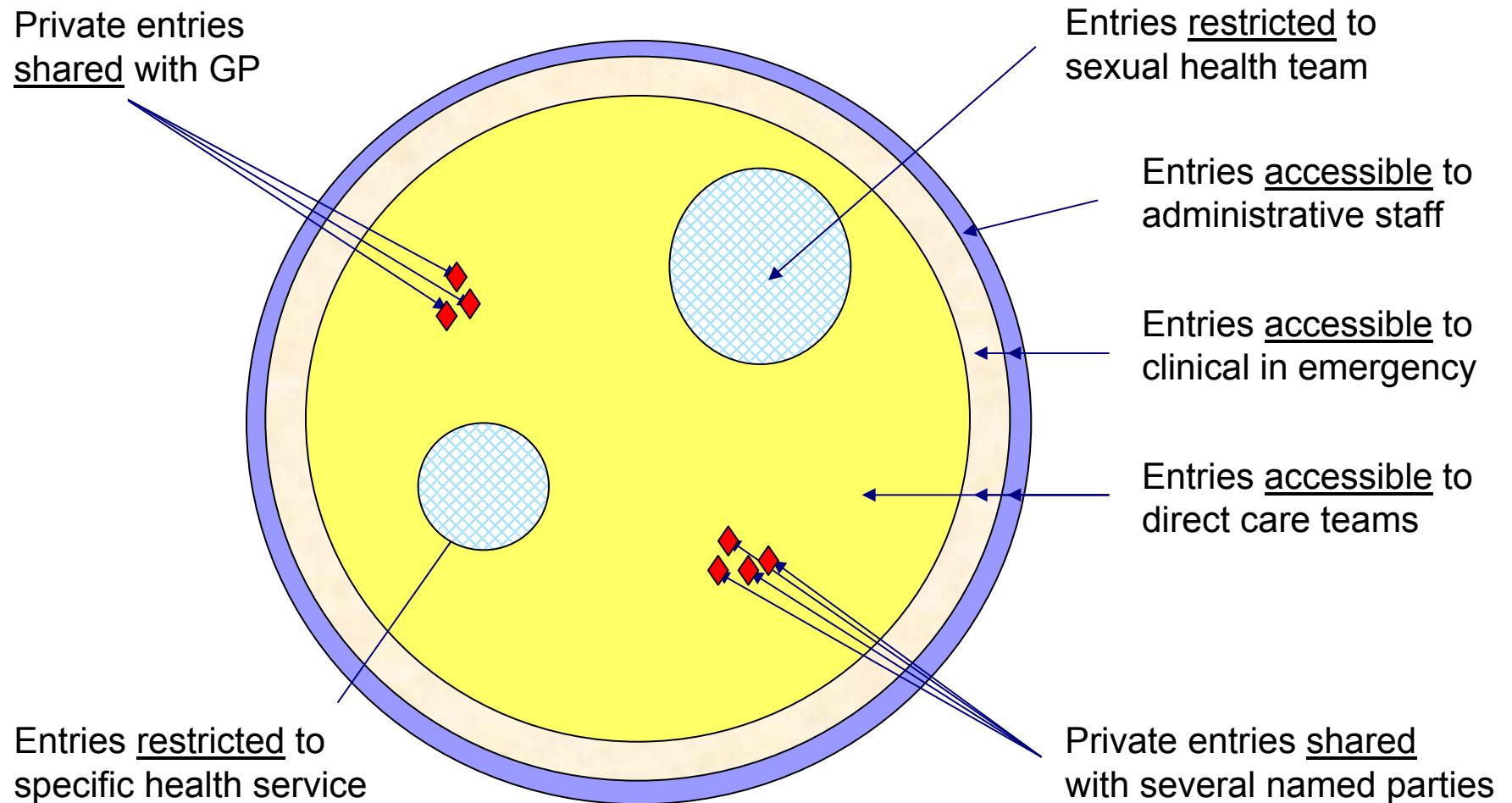
Enabling additional access (e.g., research)



Basic Consent Publication Controls



HITSP Manage Consent Directives – How does it work? **Document Accessibility**

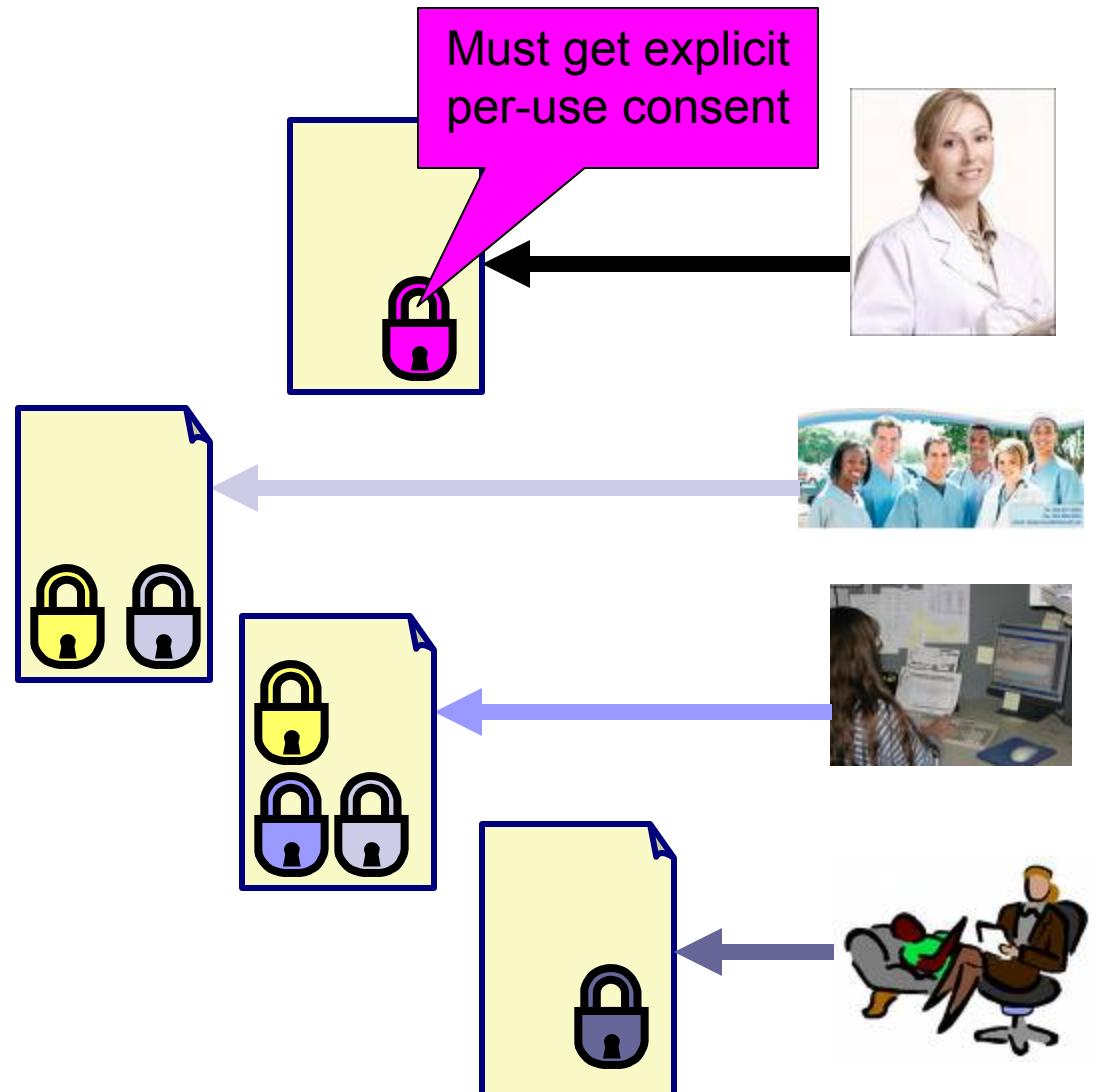
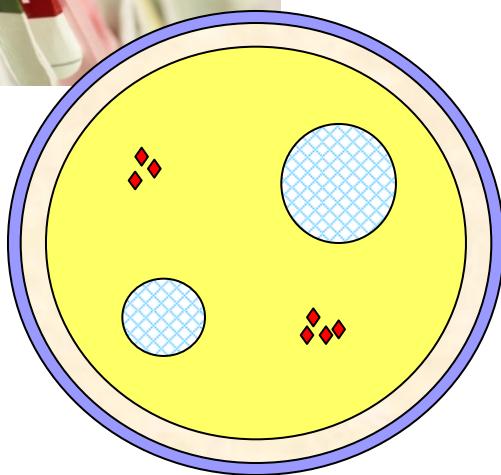


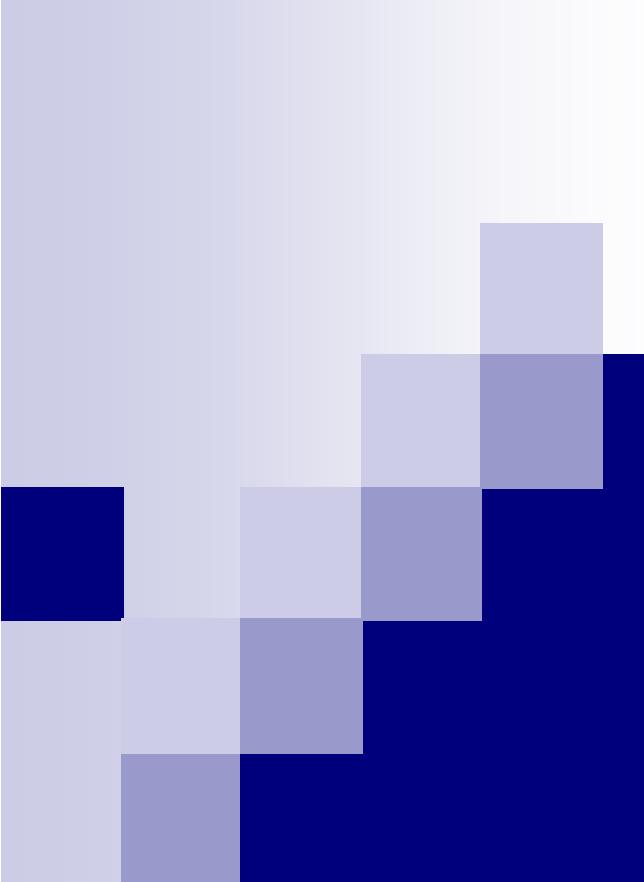
Source: Dipak Kalra & prEN 13606-4

Sample Role-based Access Control table

Sensitivity Functional Role	Mediated by Direct Care Provider	Research Information	Sensitive Clinical Information	General Clinical Information	Dietary Restrictions	Administrative Information	Billing Information
Administrative Staff							X
Dietary Staff		X	X				
General Care Provider		X	X	X			
Direct Care Provider		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”



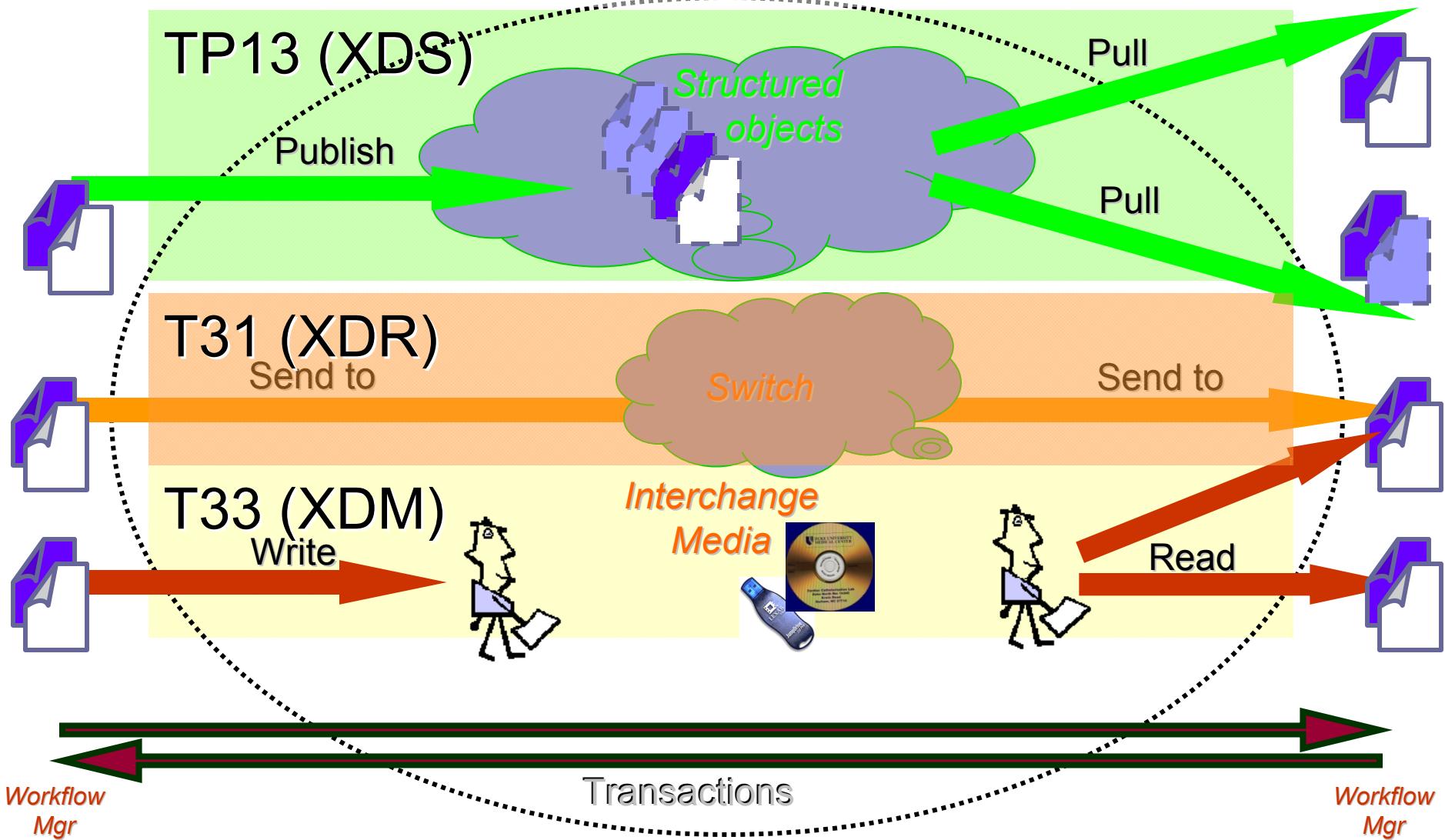


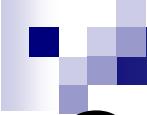
The bigger picture

Flexible Infrastructure

Sharing, Sending and Interchanging

Health Information Exchange



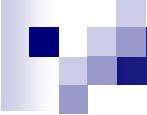


Gaps for potential future development

- Better coded vocabulary for confidentiality codes
 - Complex policies on a document-by-document basis
 - Extension to objects other than XDS (e.g., DICOM)
- Patient Access to
 - Sensitive health topics (you are going to die)
 - Low sensitivity (scheduling)
 - Self-monitoring (blood sugar)
 - Authoritative updates / amendments / removal
- Complex Privacy “consent” Policy capabilities
 - Supporting Inclusion Lists
 - Supporting Exclusion Lists
 - Exceptions and Obligations
 - Supporting functional role language
- Access Control Service
 - Centralized Policies
- Accounting of Disclosures reports, alerts, messaging
 - To support reporting to the “consumer” when their data are accessed



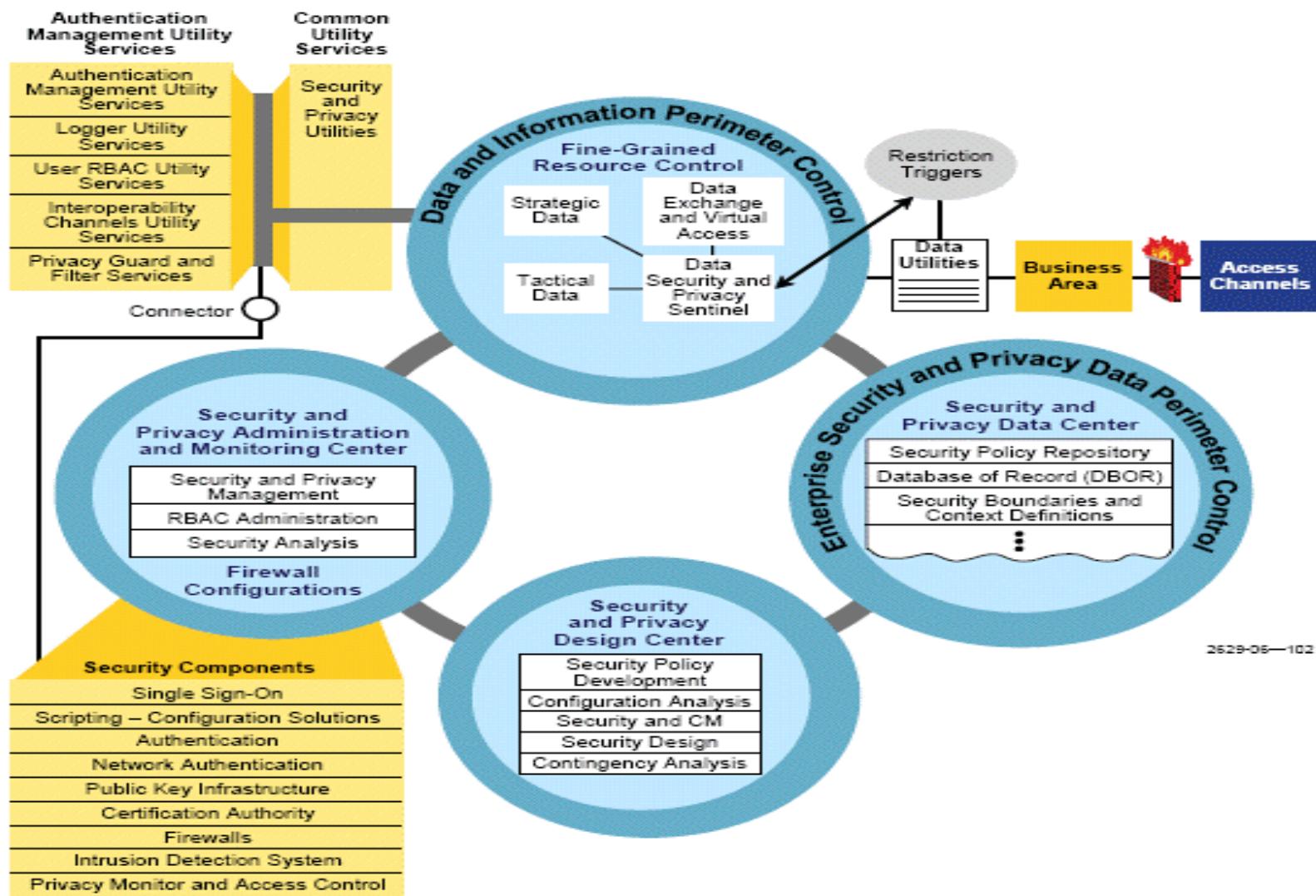
*MMIS/MITA Architecture
and Electronic Consent Directives*



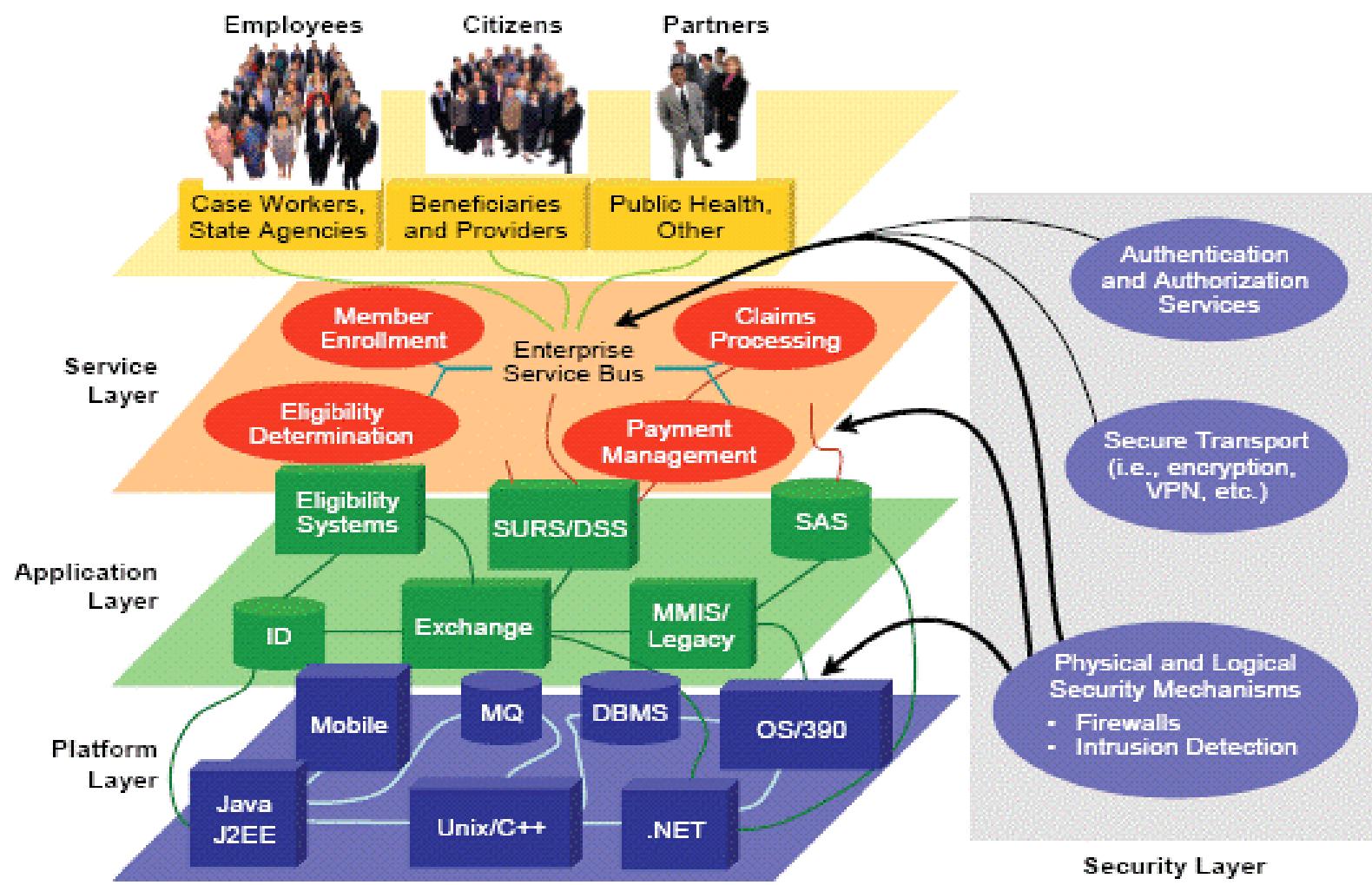
MMIS/MITA Architecture and Privacy/Security

- Technical principles of MITA include the following:
 - Security and privacy must be integrated throughout the architecture.
 - Model architecture ensures interoperability within the various system components.
 - Interoperability standards are to be established and followed.
 - Secure data exchange is to be supported and promoted.
- MITA adheres to federal HIE standards
- HITSP is developing the interoperable HIE standards for privacy and security

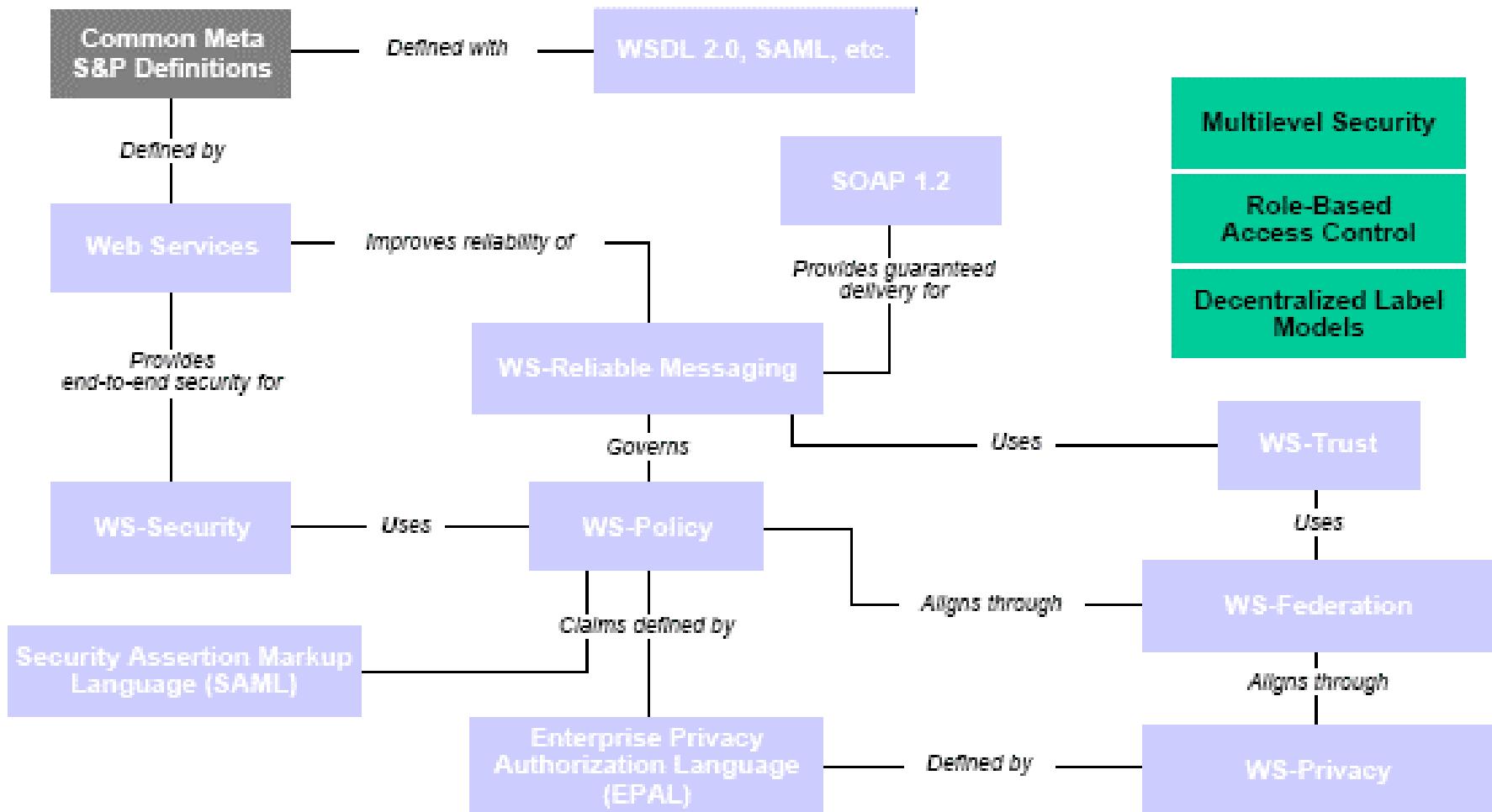
MMIS/MITA SOA Architecture: Security and Privacy Model

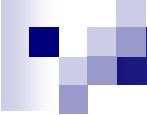


MMIS/MITA SOA Architecture: Privacy/Security Core Services



MMIS/MITA SOA Architecture: Privacy/Security Standards





Conclusion

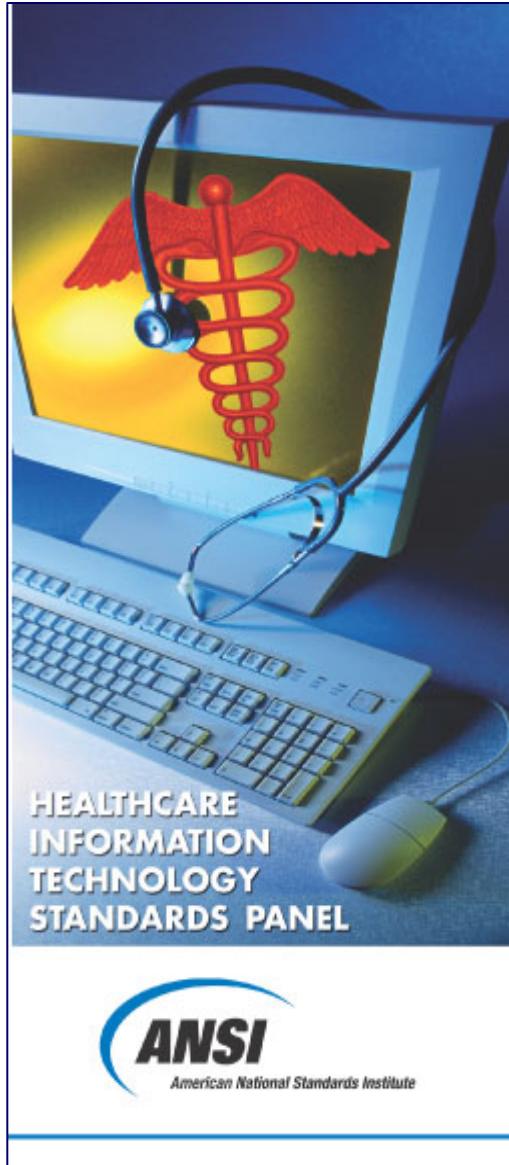
- In an era of increased Health IT adoption and HIE implementation, electronic interoperable health information privacy consent standards are much needed.
- Standards must be flexible to respond to various co-existing jurisdictional policy and program requirements.
- HITSP has provided the necessary basic privacy interoperable standards today, along with a core set of security standards that support privacy.
- Medicaid's MMIS/MITA architecture is intended to support and use national interoperable standards for privacy and security.
- Implementation testing of privacy standards within Medicaid MMIS/MITA systems can begin.
- There are still some coding gaps and room for improvements – and YOU can help!
- Medicaid should begin participating more actively in HITSP harmonization efforts.



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.



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



Q&A





Contact Information

- For additional questions on this topic,
please contact:
 - Johnathan Coleman – jc@securityrs.com
 - John Moehrke – John.Moehrke@med.ge.com
 - Walter Suarez – walter.suarez@sga.us.com

Comments and Recommendations for Future Sessions

- Please send your comments and recommendations for future sessions to the project's e-mail address:

Medicaid-SCHIP-HIT@ahrq.hhs.gov

Project Information

Please send comments and recommendations to:

Medicaid-SCHIP-HIT@ahrq.hhs.gov

or call toll-free:

1-866-253-1627

Medicaid-SCHIP-HIT@ahrq.hhs.gov

<http://healthit.ahrq.gov>