

# OASIS-HITSP

## Privacy Consent and Access Control

### Advanced Technology Demonstration

Chicago  
McCormick Place  
April 4-8 2009

Duane DeCouteau (Edmond Scientific)  
[Duane.DeCouteau@VA.gov](mailto:Duane.DeCouteau@VA.gov)

Johnathan Coleman (Security Risk Solutions, Inc.)  
[JC@securityrs.com](mailto:JC@securityrs.com)

Organization for the Advancement of Structured Information Standards

Healthcare Information Technology Standards Panel





# Interoperability Showcase

## Presents

An

Advanced technology demonstration of Health and Human Services recognized privacy and access controls for the secure electronic exchange of healthcare information.

**Booth 7750**

### **RSA Conference April 2008**

Multi-vendor demonstration of OASIS XACML supporting HITSP TP20

### **London Conference Oct 2008**

Extensions to the RSA demonstration

### **HIMSS Apr 2009**

End-to-end demonstration of OASIS SAML/ XACML/ WS-Trust supporting HITSP TP20/30

# Privacy—Security's Point of Pain

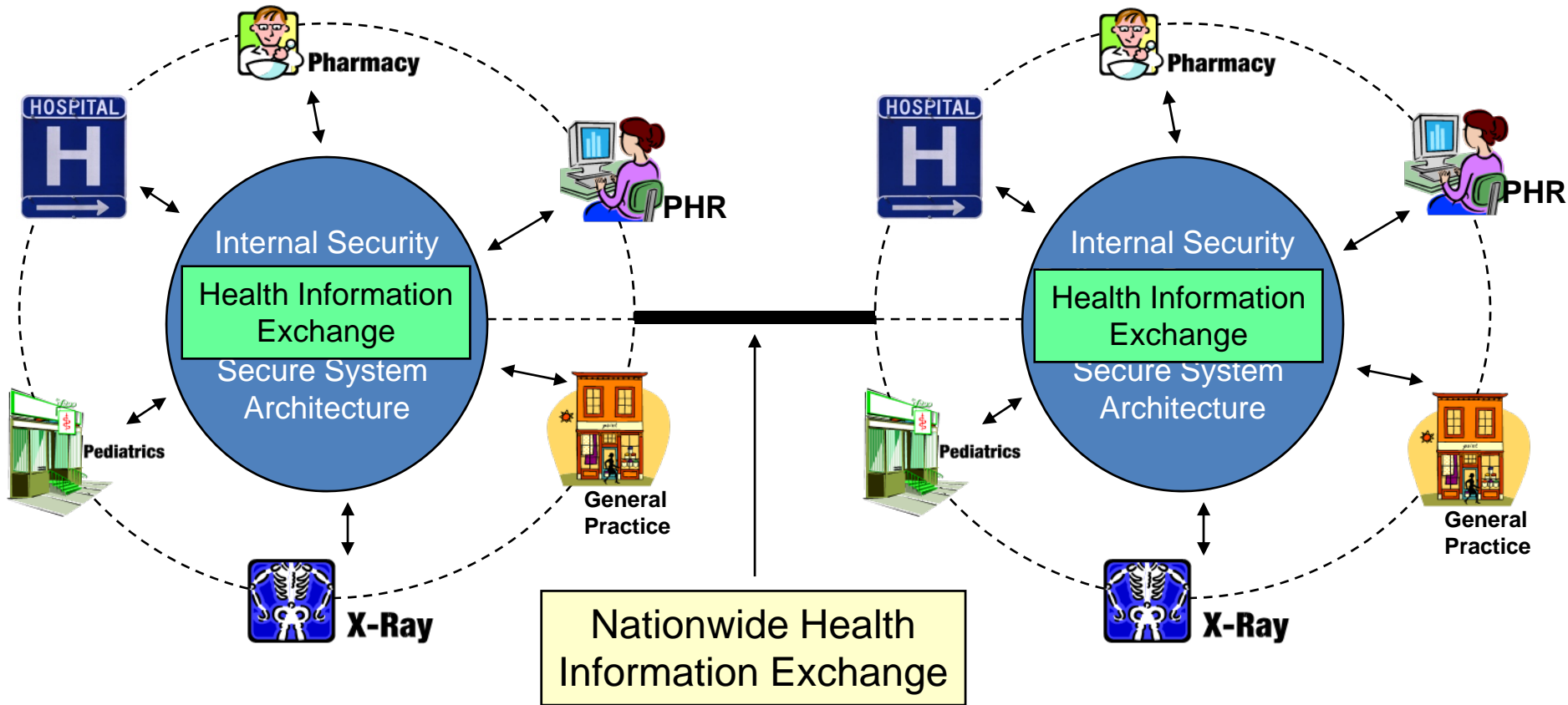
- **Privacy Traditionally not a Security concern-Now it is**
  - Security administrators unfamiliar with Privacy
  - Privacy Coordinators unfamiliar Security systems
- **Health Information Exchange “Opt in/Opt out”**
  - Too coarse
  - Patients want more options and control
- **Privacy complicates, conflicts with traditional rules**
  - E.g. DURSA complicates data sharing for federal providers
- **HIPAA Privacy Rule-Too complex for information systems?**
- **Managing and enforcing consumer consents for disclosure of data**
  - To what granularity?
  - Impact of patient decisions on provision of care?

# Status of Security and Privacy

## Where are We Now?

- Vendor security/privacy products are available
- HITSP Constructs are mature (DHHS Recognized)
- OASIS – HITSP demonstrations since April 2008
- NHIN demonstrations have been done
- Core Interoperability Standards/Profiles are there, others are in the pipeline

# Interoperability – The Focus of HITSP

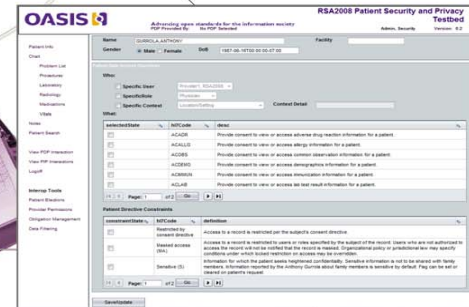


# Security and Privacy Demonstration Overview: Provision of Care

## Integrating Systems and People



**Patient Consent**



Care and Treatment



**HIS Security Policy**



**Clinical Roles and  
Permissions**

**Using OASIS Standards to  
Enforce Privacy Consents  
and Access Control**

Information Technology Security  
Management

# Security and Privacy Demonstration Overview: Foundations

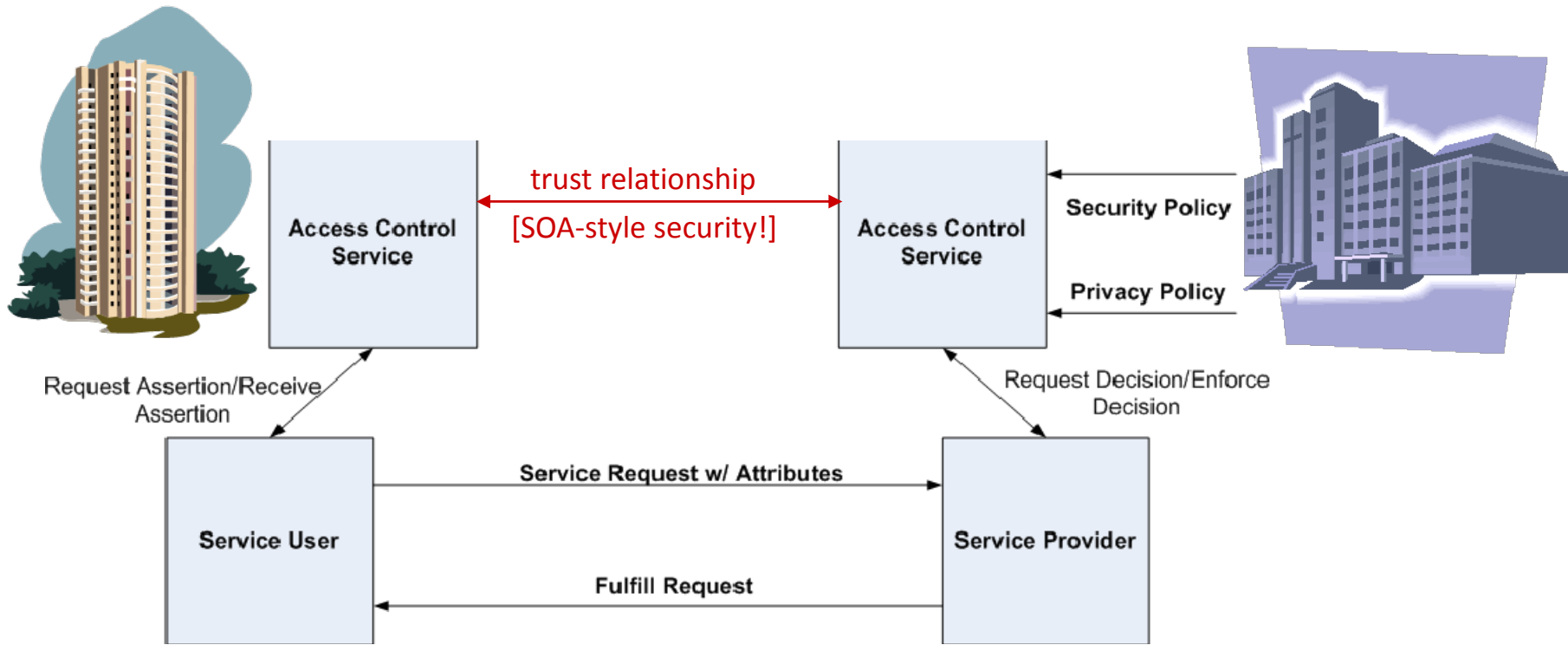
HITSP TP 20 Access Control Transaction Package describes a framework for cross-enterprise authorization interoperability in healthcare data exchange. It provides the mechanism for security authorizations which control the enforcement of security policies, including access control and the execution of consent directives.

HITSP TP 30 Manage Consent Directives Transaction Package describes a framework for capturing, managing and communicating consumer privacy preferences and consent.

XSPA Profiles of OASIS standards describes a minimum set of subject and resource attributes necessary to support cross-enterprise access control decisions between two Healthcare organizations.



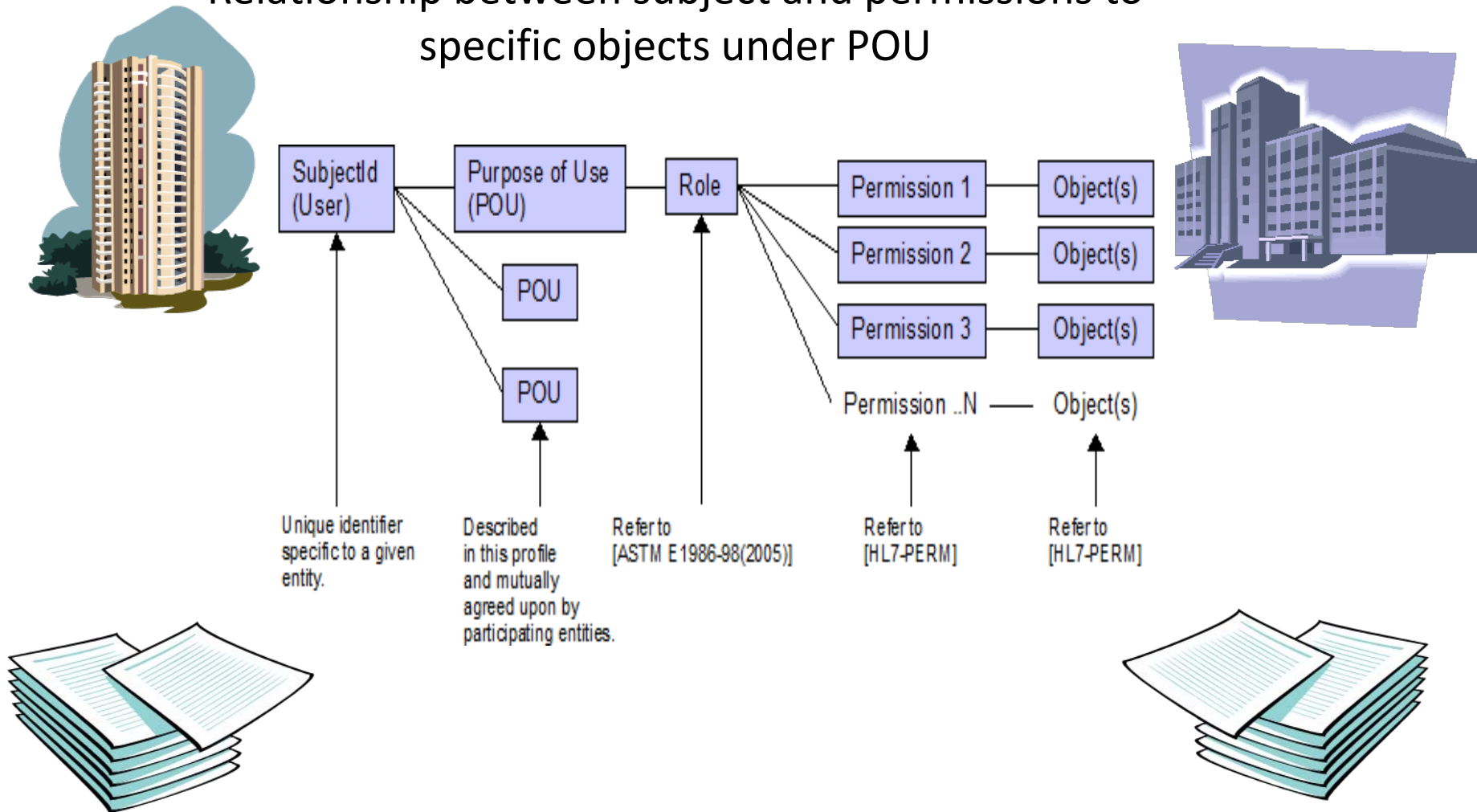
# Security and Privacy Demonstration Overview: Cross Enterprise Data Sharing



**XSPA SAML Profile / HITSP TP20 High-Level Interactions**

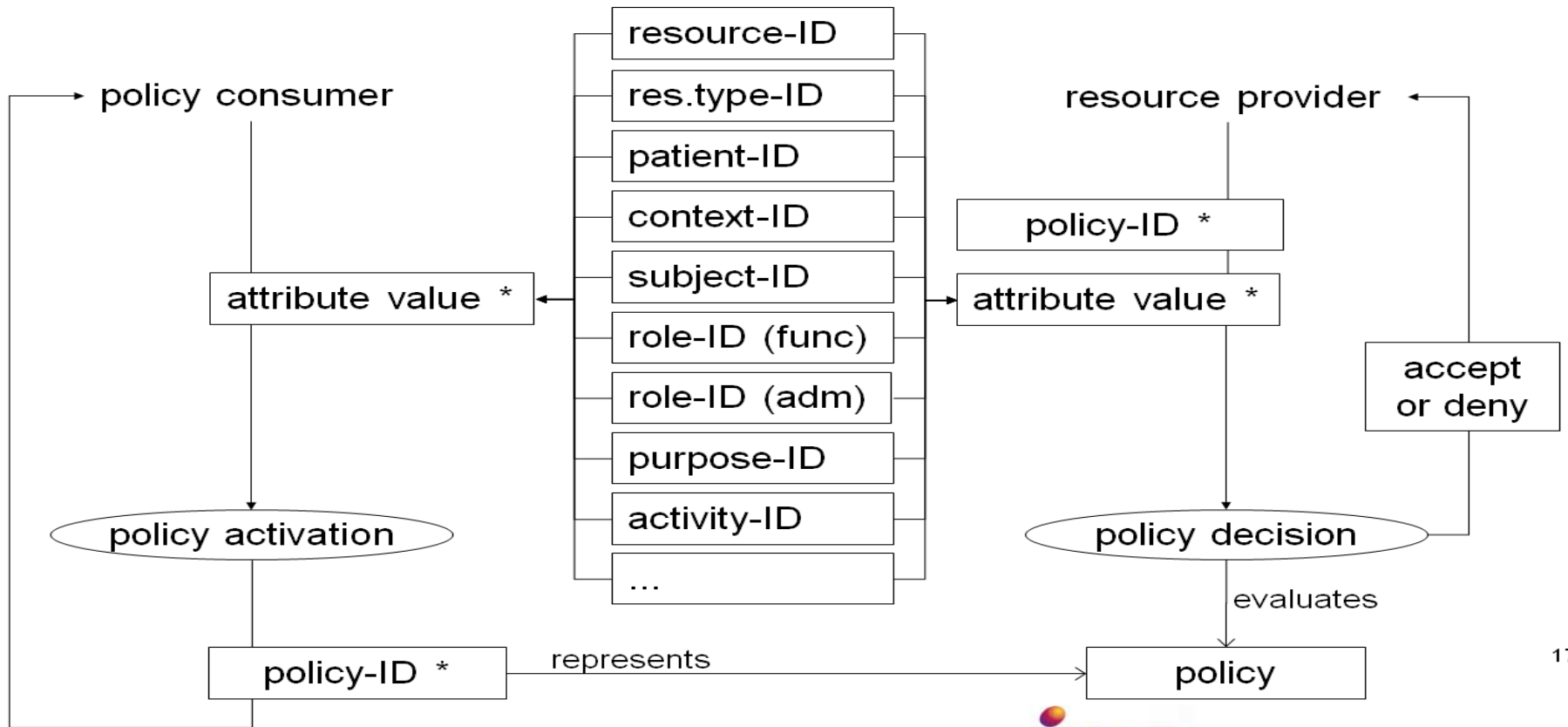
# Security and Privacy Demonstration Overview: Behind the Scenes

Relationship between subject and permissions to  
specific objects under POU



# Security and Privacy Demonstration Overview: Shared Policies and Attributes

## Attributes and Policies



17



- **Demonstrate the Enforcement of Patient Consent Directives**
  - Opt-In / Opt-Out
  - Allowed Organizations
  - Confidentiality Codes (Consent Directive Template)
  - Deny Access based on Role and Purpose of Use
  - Deny Access to Specific Providers
  - Masked Results based on Role
  - Masked Results for Specific Providers
  
- **Demonstrate the Enforcement of Organizational Policies**
  - Limit access to specific organizations
  - Limit access during specific hours of the day
  - Require certain roles based on purpose of use and service requested
  - Require certain permissions based on purpose of use and service requested

Select for Cross-domain Request of clinical summary

If access control decision is DENY  
User may assert Purpose of Use as Emergency Treatment.

Select to Perform Cross-domain patient discovery

If DENIED message will appear here.

Clinical Summary from Domain B

The screenshot shows the XSPA web application interface. At the top, it displays 'Security and Privacy Authorization Testbed' and 'Version: 2.0'. The user is identified as 'Doctor, Bob' in 'Healthcare Domain A'. The patient information section shows 'Name: SMITH, BAMBI', 'Gender: Female', and 'DoB: 1952-06-25T00:00:00-07:00'. Below this is a table with columns: Last Name, First Name, Gender, Date of Birth, Organization, View Consent, and View Policy. The table contains one row for 'SMITH, BAMBI, F, 19520625, Healthcare Domain B'. A 'Declare Emergency' button is visible on the right. The main content area is titled 'Department of Defense SUMMARIZATION OF EPISODE NOTE' and contains patient details: 'PATIENT: BAMBI SMITH', 'ADDRESS: 123 ANYPLACE DR, ANY CITY USA, ANYSTATE 12345', 'BIRTHDATE: 25-JUN-52', 'SEX: Female', and 'LANGUAGES: English (US)'. A 'Table of Contents' section is also present. The left sidebar contains navigation options like 'Chart', 'Problem List', 'Procedures', 'Laboratory', 'Radiology', 'Medications', 'Vitals', 'Notes', 'Patient Search', 'Local PDP Interaction', 'Local PJP Interactions', 'Cross-Domain Search', 'View XSPA Messages', 'Logoff', 'Interop Tools', 'Patient Elections', 'User Based Access', 'Masked Access', and 'Provider Permissions'. The bottom of the page features the 'HITSP OASIS' logo.

The screenshot displays the XSPA web application interface. At the top, the XSPA logo and title are visible. The main content area shows a patient's information: Name (SMITH, BAMBI), Facility (Healthcare Domain B), Gender (Female), and Date of Birth (19520625). Below this, there are tabs for Patient Participation, Allowed Organizations, Confidentiality, Control Access to Providers, Control Access to Objects, and View Directive. The 'Control Access to Providers' tab is active, showing a table with columns for Structured Role and Purpose of Use. The table lists 'Pharmacist' for 'Healthcare Treatment'. A red box highlights the 'Limit Access by Role' section, which allows patients to deny access based on their ASTM role and purpose of use. A red arrow points from this box to the 'Limit Access by Role' tab. Another red box highlights the XACML policy URI: urn:oasis:names:tc:xspa:1.0:resource:patient:dissenting-role. Below the table, there are dropdown menus for Purpose of Use (Healthcare Treatment) and Structured Role (Administration - Health Records (Medical Records)/Health Information Management Department), along with Add, Delete, and Reset buttons. The left sidebar contains a navigation menu with categories like Consent Directive Exchange, Organizational Constraints, Patient Constraints, and XSPA Vocabulary. The bottom left corner features the HITSP OASIS logo and contact information for the Veterans Health Administration, DoD Naval Health Research Center.

**Limit Access by Role**  
Allows patient ability to DENY Access Based on a users ASTM Role and Purpose of Use.

Structured Role	Purpose of Use
Pharmacist	Healthcare Treatment

Click on Structured Role to select.

These are evaluated in the XACML policies as;  
urn:oasis:names:tc:xspa:1.0:resource:patient:dissenting-role

**Purpose of Use:** Healthcare Treatment

**Structured Role:** Administration - Health Records (Medical Records)/Health Information Management Department

Add Delete Reset

The screenshot shows the XSPA web application interface. The browser address bar displays two URLs: `http://67.52.150.106/XS...` and `http://204.115.177.218/XA...`. The page title is "HIMSS 2009 Patient Consent Directive and Organizational Policy Kiosk" with "Version 1.0" below it. The XSPA logo and name are in the top left. A navigation menu on the left includes "Directive Services" (with sub-items "View Real-time Activity" and "XSPA Message Traffic"), "Organizational Constraints" (with sub-items "Allowed Healthcare Organizations", "Hours of Operations", "Required Roles", "Required Permissions"), "Patient Constraints" (with sub-items "Patient Selection", "Consent Directives"), and "XSPA Vocabulary" (with sub-items "ASTM Roles", "HL7 Confidentiality Codes", "HL7 Permissions Catalog", "Purpose Of Use"). The main content area shows a patient profile for "SMITH, BAMBI" at "Healthcare Domain B", with gender "Female" and date of birth "19520625". Below this are tabs for "Patient Participation", "Allowed Organizations", "Confidentiality", "Control Access to Providers", "Control Access to Objects", and "View Directive". The "Deny Object Access by Provider" tab is active, displaying a table with columns "NPI", "Provider Name", "Primary Location", and "Healthcare Object". The table contains two entries: NPI 100027 for Doctor, Charlie S at Facility B for Medications, and NPI 100036 for Doctor, Alice at Healthcare Domain A for Problems. A red box highlights the text "Deny Object Access by Provider" and "Allows the patient to DENY access to specific Healthcare objects to specific Providers." with arrows pointing to the table header and the second row. Below the table is a form with fields for "Provider Name" (set to "Doctor, Bob H"), "NPI", "Location", and "Healthcare Object" (set to "Alerts"). There are "Add", "Delete", and "Reset" buttons. A red box highlights the text "These are evaluated in the XACML policies as; urn:oasis:names:tc:xspa:1.0:resource:patient:masked:'healthcareobject':dissenting-subject-id" with an arrow pointing to the table. The bottom left features the HITSP OASIS logo and text: "Veterans Health Administration, DoD Naval Health Research Center, Sun Microsystems, Red Hat, Jericho Systems".

**Deny Object Access by Provider**  
Allows the patient to DENY access to specific Healthcare objects to specific Providers.

NPI	Provider Name	Primary Location	Healthcare Object
100027	Doctor, Charlie S	Facility B	Medications
100036	Doctor, Alice	Healthcare Domain A	Problems

Click on NPI to select.

These are evaluated in the XACML policies as;  
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:'healthcareobject':dissenting-subject-id

Provider Name: Doctor, Bob H      NPI:      Location:      Healthcare Object: Alerts

Add      Delete      Reset

## Service Provider – Vocabulary

ASTM 1986 Roles

Role ID	Friendly Name	URN	Code System
44	Administration - Health Records (Medical Records)/Health Information Management Department	urn:oid:1.2.840.113583.1.2.2.44	ISO
45	Administrative Department - Administrative Support Staff and Services	urn:oid:1.2.840.113583.1.2.2.45	ISO
57	Administrative Department - File Clerk	urn:oid:1.2.840.113583.1.2.2.57	ISO
61	Administrative Department - Supervisory Personnel	urn:oid:1.2.840.113583.1.2.2.61	ISO
65	Administrative Support - Health Records (Medical Records)/Health Information Management Department	urn:oid:1.2.840.113583.1.2.2.65	ISO
62	Administrative Support Personnel	urn:oid:1.2.840.113583.1.2.2.62	ISO
80	Administrative Support Staff	urn:oid:1.2.840.113583.1.2.2.80	ISO

HL7 Permission Catalog

Code ID	Consent Code	Description	URN
4	ISA	Access to a record is restricted to users or roles specified by the subject of the record. Users who are not authorized to access the record will not be notified that the record is restricted. Organizational policy or jurisdictional law may specify conditions under which locked restriction on access may be overridden.	urn:oid:1.2.840.113583.1.2.2.4
5	S	Information for which the patient seeks heightened confidentiality. Sensitive information is not to be shared with family members. Information reported by the patient about family members is sensitive by default. Flag can be set or cleared on patient's request.	urn:oid:1.2.840.113583.1.2.2.5

HL7 Confidentiality Codes

Permission ID	Healthcare Object	Action	Permission	URN	Code System
1	Medical History	Read	PRD-003	urn:oid:2.16.840.1.113583.1.2.2.1	HL7
2	Vital signs/Patient Measurements	Read	PRD-006	urn:oid:2.16.840.1.113583.1.2.2.2	HL7
3	Patient Identification and Lookup	Read	PRD-008	urn:oid:2.16.840.1.113583.1.2.2.3	HL7
4	Patient Medications	Read	PRD-010	urn:oid:2.16.840.1.113583.1.2.2.4	HL7
5	Past Visits	Read	PRD-012	urn:oid:2.16.840.1.113583.1.2.2.5	HL7
6	Progress Notes	Read	PRD-017	urn:oid:2.16.840.1.113583.1.2.2.6	HL7

Purpose of Use

ID	Value	URN
1	Healthcare Treatment	urn:oid:1.2.840.113583.1.2.2.1
2	Payment and Operations	urn:oid:1.2.840.113583.1.2.2.2
3	Emergency Treatment	urn:oid:1.2.840.113583.1.2.2.3
4	System Administration	urn:oid:1.2.840.113583.1.2.2.4
5	Research	urn:oid:1.2.840.113583.1.2.2.5
6	Marketing	urn:oid:1.2.840.113583.1.2.2.6
7	Public Health	urn:oid:1.2.840.113583.1.2.2.7
8	Programmer Access	urn:oid:1.2.840.113583.1.2.2.8

# Summary of Technical Features

- DHHS approved HITSP IS, standards, constructs (TP20/TP30)
- DHHS Security and Privacy Framework Compliant
- HIPAA Security and Privacy Compliant
- Extends Security and Privacy technologies for NHIN
- Standard Clinical Roles (ASTM, ANSI, HL7)
- Standard Patient Consent Directives (HL7, IHE BPPC)
- Standard Web-Service Protocols (OASIS SAML, XACML, WS-Trust)
- Federation of authenticated identities (OASIS SAML, IHE XUA, C19)
- Standard Interoperability Profiles (OASIS XSPA, IHE)
- Implementation-ready without change to legacy systems
- Policies managed centrally, enforced locally (ASTM, ISO PMI)
- Vendor supported solutions

IS = Interface Specification

NHIN = Nationwide Health Information Network

PMI = Privilege Management Infrastructure

SAML=Security Assertion Markup Language

XACML= eXtensible Access Control Markup Language

C19 = HITSP Entity Identity Assertion Component



# Ongoing Standards Work

- **HL7 Standards**
  - Update to Roles (adding new vocabulary from SNOMED CT, LOINC, ICD-10)
  - Joint Security and Privacy Information Models
  - Update to Consent Directives
- **OASIS**
  - XSPA Profiles
  - WS-Federation
- **Conformance Testing at the IHE Connectathon**

ICD=International Classification of Diseases

LOINC=Logical Observation Identifiers, Names, and Codes

SNOMED CT=Standard Nomenclature of Medical Diseases and Operations-Clinical Terms



# Conclusion

**Health and Human Services Security and Privacy Framework is realizable**

**We are Ready**

- Vendor security/privacy products are available
- HITSP Constructs are mature (DHHS Accepted)
- OASIS – HITSP demonstrations since April 2008
- NHIN demonstrations have been done
- Interoperability Standards/Profiles are there

## Working to Meet the Privacy Needs of the Nation Today



Jericho Systems Corporation



Red Hat



Sun Microsystems



U.S. Department of Defense



U.S. Department of Veterans Affairs