HIMSS 2009 Playbook

HITSP

OASIS

TP/20 describes framework for cross-enterprise authorization interoperability in healthcare data exchange.

XSPA Profiles describe a minimum set of subject and resource attributes necessary to perform a cross-enterprise access control decision between two Healthcare organizations.

Interop Story

- Demonstrate the Enforcement of Patient Consent Directives
  - Opt-In / Opt-Out
  - Allowed Organizations
  - Confidentiality Codes (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
  - Required certain roles based on purpose of use and service requested
  - Require certain permissions based on purpose of use and service requested

Interop Story

SERVICE USER (REQUESTOR)

•Domain A – the TP20 Service User (Requestor), is not a production system but is representative of a light Electronic Health Record or Provider Portal
• The requestor is representative of a legacy implementation that has been TP20 enable and supports the cross-domain dialogue between healthcare organizations as described by the XSPA profiles of SAML and WS-TRUST
•It has it's own internally roles and permissions and Access Control System based on XACML Interops of RSA2008 and Ditton Manor London England (Sun Microsystems provide ACS)

SERVICE PROVIDER (RESPONDER)

•Domain B – the TP20 Service Provider (Responder), is representative of a production implementation at a component level, i.e., Service Provider, Assertion Handler, PEP,PIP,PDP, Attribute Services, and Data Masking Subsystem
•Domain B – Understand how to consume and produce an access control decision based on the XSPA Profiles of SAML and WS-TRUST
•It offers 2 services – patient discovery and getMedicalRecord which returns the opted-in clinical summary
•The Domain B Service provider wraps, or TP20 enables, a DoD developed Document Assembler from the December demostrations of NHIN (this was an implementation specific decision, the Service provider could just as easily wrap the NHIN Federal Adapter

Participant Technologies

Jericho Systems and Red Hat

1) Implement the XSPA Profile of XACML
2) Control all aspects of PHI data delivery outside of the Domain B Healthcare Enterprise
3) Share and consume a common XACML Policy

Sun Microsystems

1) Delivers standard based interface libraries to produce XACML request and consume its response
2) Provide Circle of Trust for PDPs that conform to the XSPA Profile of XACML

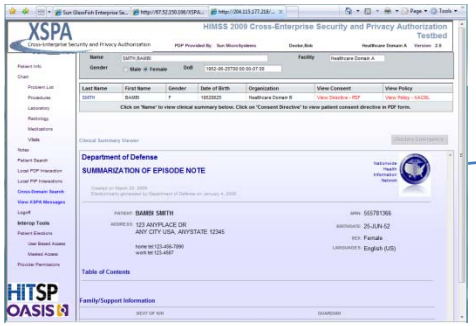
Dept. of Veterans Affairs

1) Delivers the TP20 Service Provider wrapper/enabler
2) Provides ability to consume a Subject and Resource assertion as described by XSPA Profiles of SAML and WS-TRUST
3) Provides ability to augment Subject and Resource assertion with organizational policies and patient consent directives
4) Provides Enforcement of PDP decision
5) Delivers Obligations to Service Provider

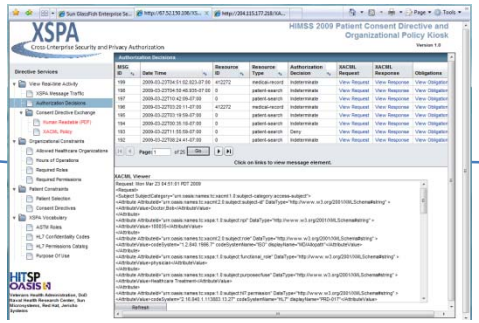
Dept. of Defense Naval Health Research Center

1) Integrate with TP20 Service Provider
2) Generate and deliver NHIN C32 Compliant Clinical Summary
3) Consume and Enforce Data Masking obligations from TP20 Service Provider

TESTBED TOPOLOGY



XSPA Profiles
of
SAML and WS-Trust



XSPA Profile
of
XACML

HITSP TP/20 – Service User

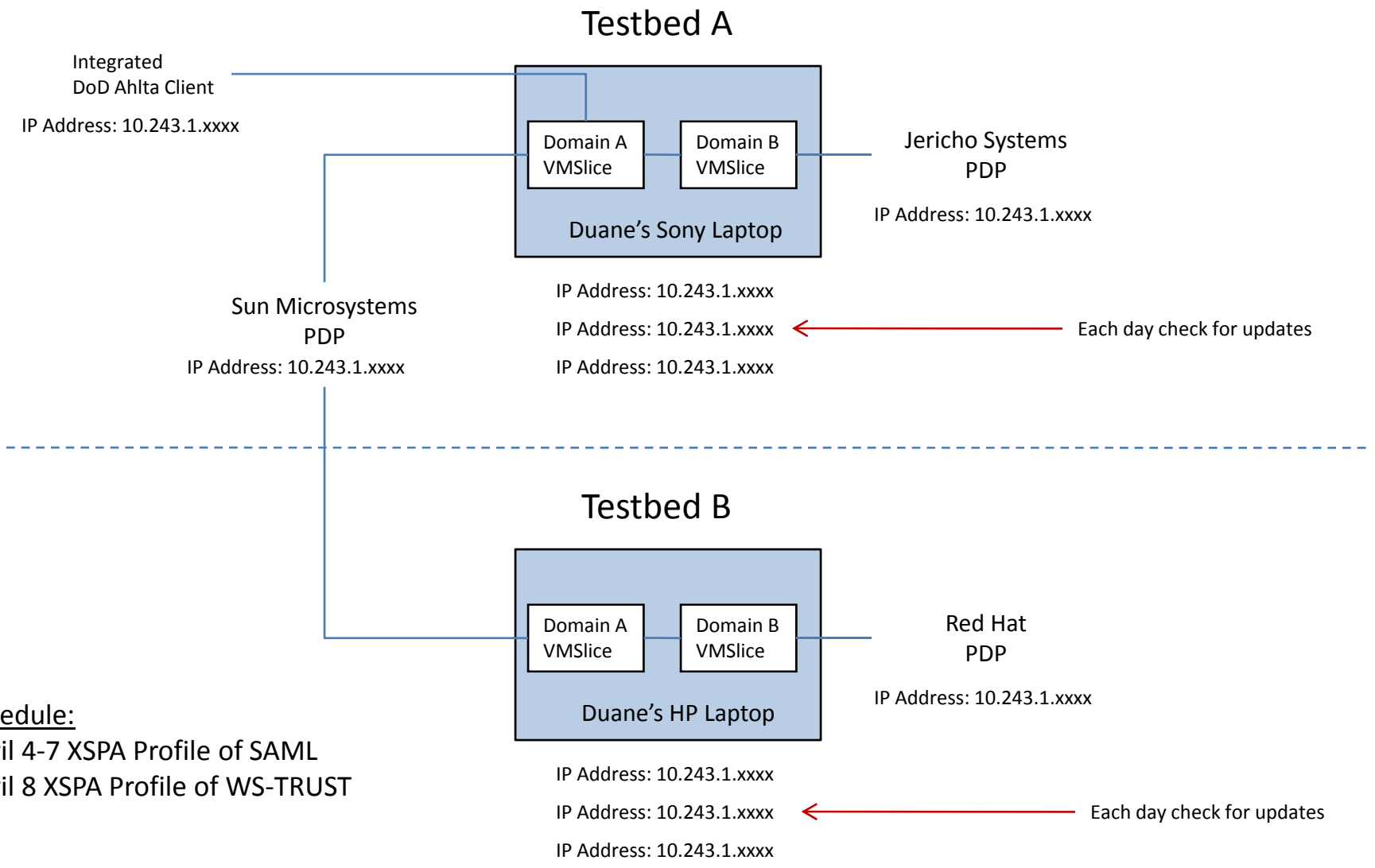
http://10.243.1.xxx/XACMLPatientPrivacy

HITSP TP/20 – Service Provider

http://10.243.1.xxx/XSPASecurityServices

HIMSS Patient Privacy and Access Control Advanced Technology Demonstration

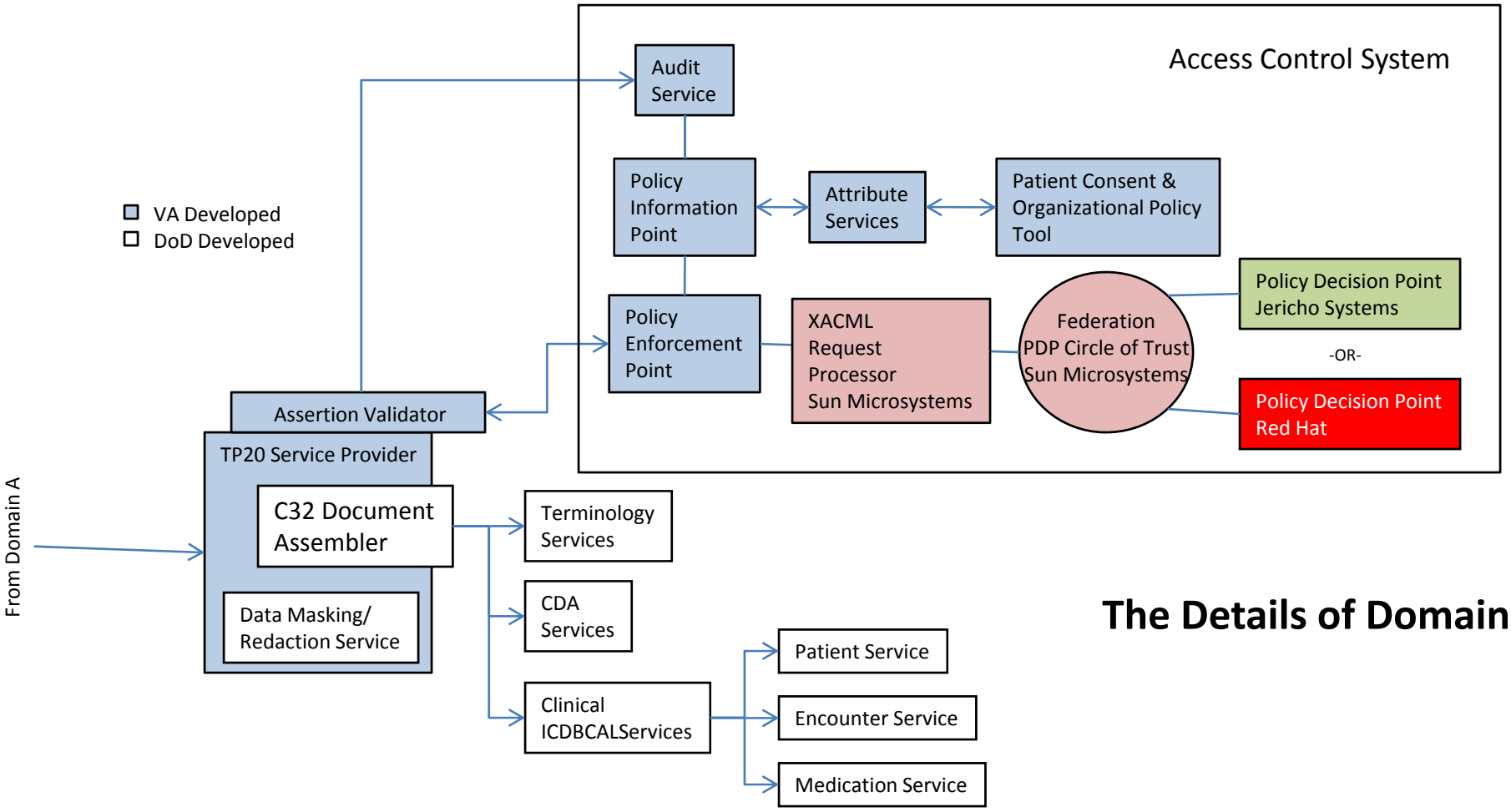
TESTBED TOPOLOGY



Schedule:
April 4-7 XSPA Profile of SAML
April 8 XSPA Profile of WS-TRUST

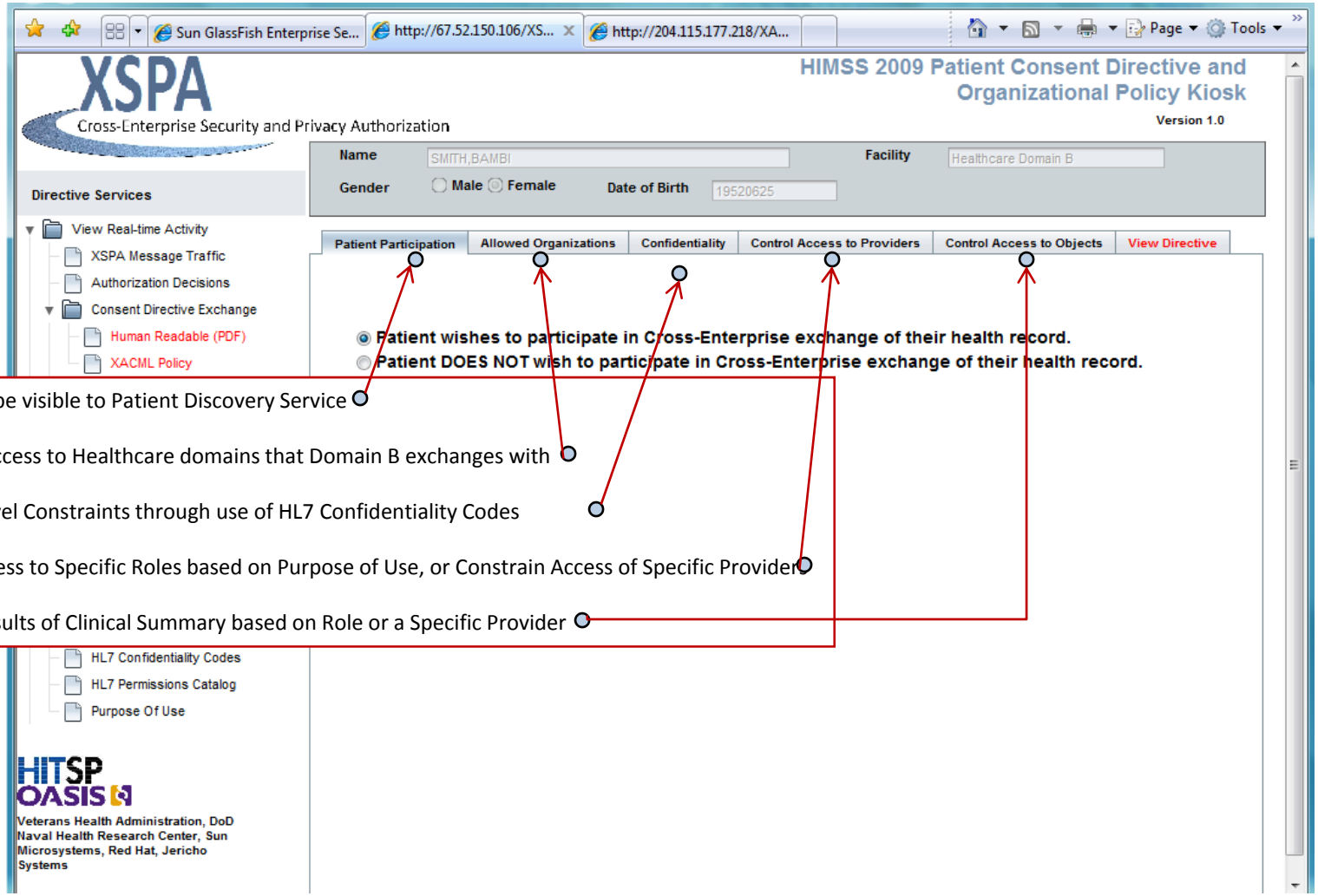
HIMSS Patient Privacy and Access Control Advanced Technology Demonstration

TESTBED TOPOLOGY



The Details of Domain B

Patient Consent Directive



Patient Must Opt-In To be visible to Patient Discovery Service

Patient Can Constrain access to Healthcare domains that Domain B exchanges with

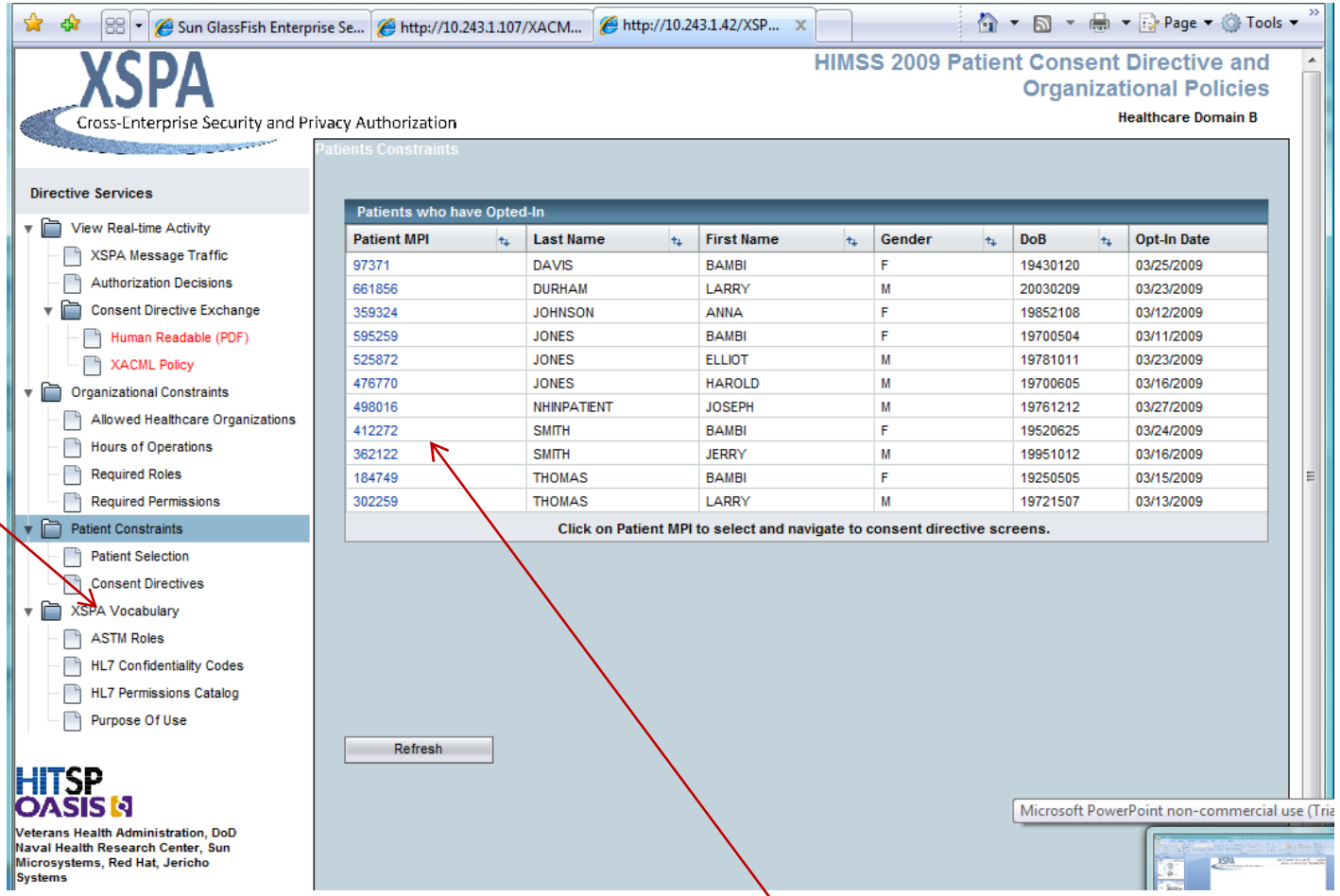
Patient Can Set High Level Constraints through use of HL7 Confidentiality Codes

Patient Can Control Access to Specific Roles based on Purpose of Use, or Constrain Access of Specific Providers

Patient Can MASKED results of Clinical Summary based on Role or a Specific Provider

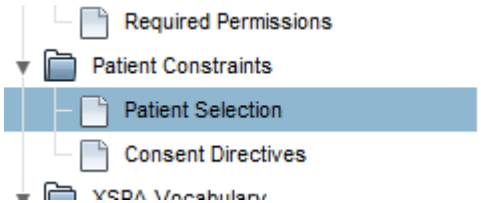
PATIENTS WHO ALREADY OPTED-IN

1) Click on the "Patient Consents" tree node a list of those patient who have opted-in will appear.



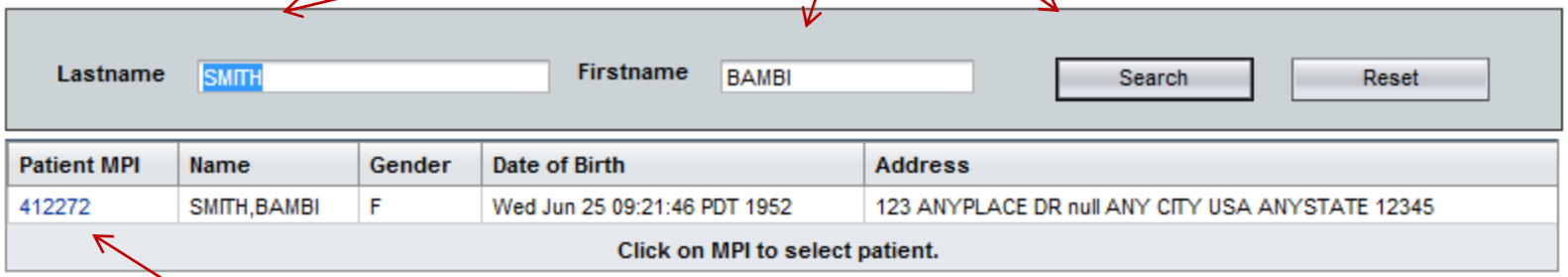
2) Select PATIENT by clicking on Their MPI link. This will direct you To the Patient Consent Directive Screens.

Add New Patient Consent Directive Opt-In - #1



1) Click on PATIENT SELECTION

2) ENTER IN LASTNAME AND FIRSTNAME CLICK ON SEARCH

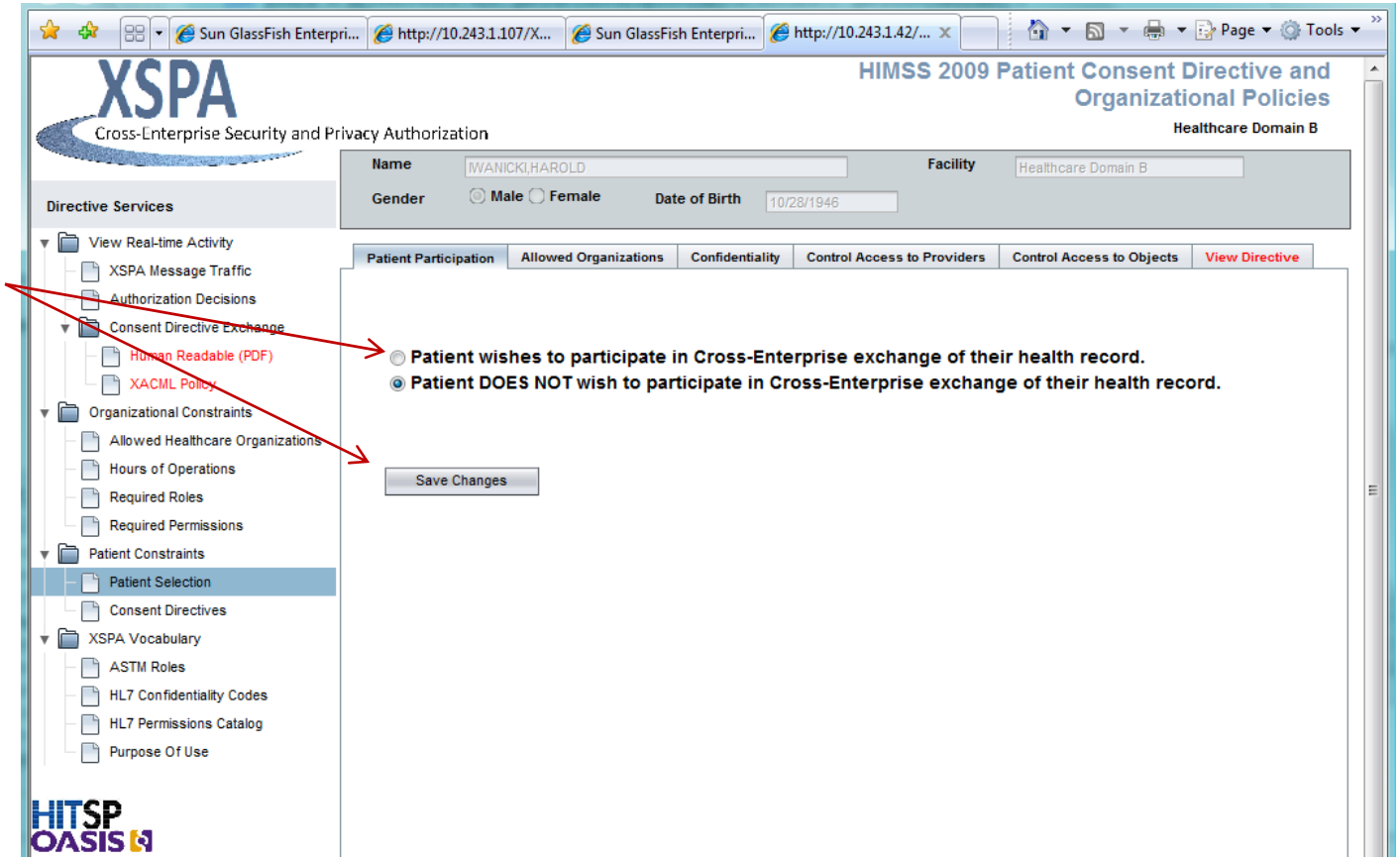


3) CLICK ON MPI, THIS SELECTS PATIENT AND NAVIGATE YOU TO PATIENT CONSENT DIRECTIVE SCREENS

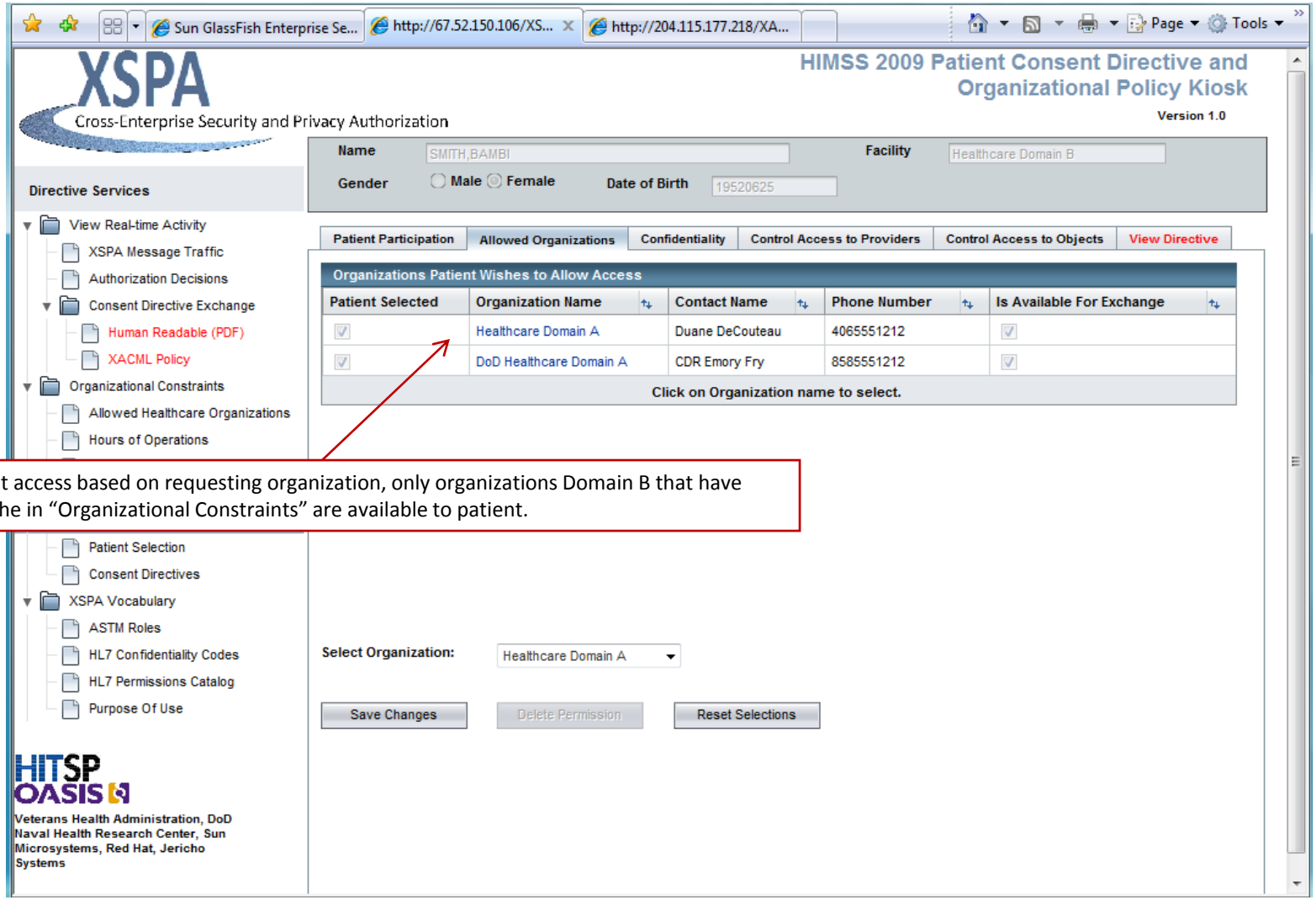
Add New Patient Consent Directive Opt-In - #2

1) Click on Option "Patient wishes…
2) Click on Save Changes to commit

3) Note: the inverse is true to Opt-Patient out. Their patient consent directive if it exist is not deleted, so opting back in restore previous state.

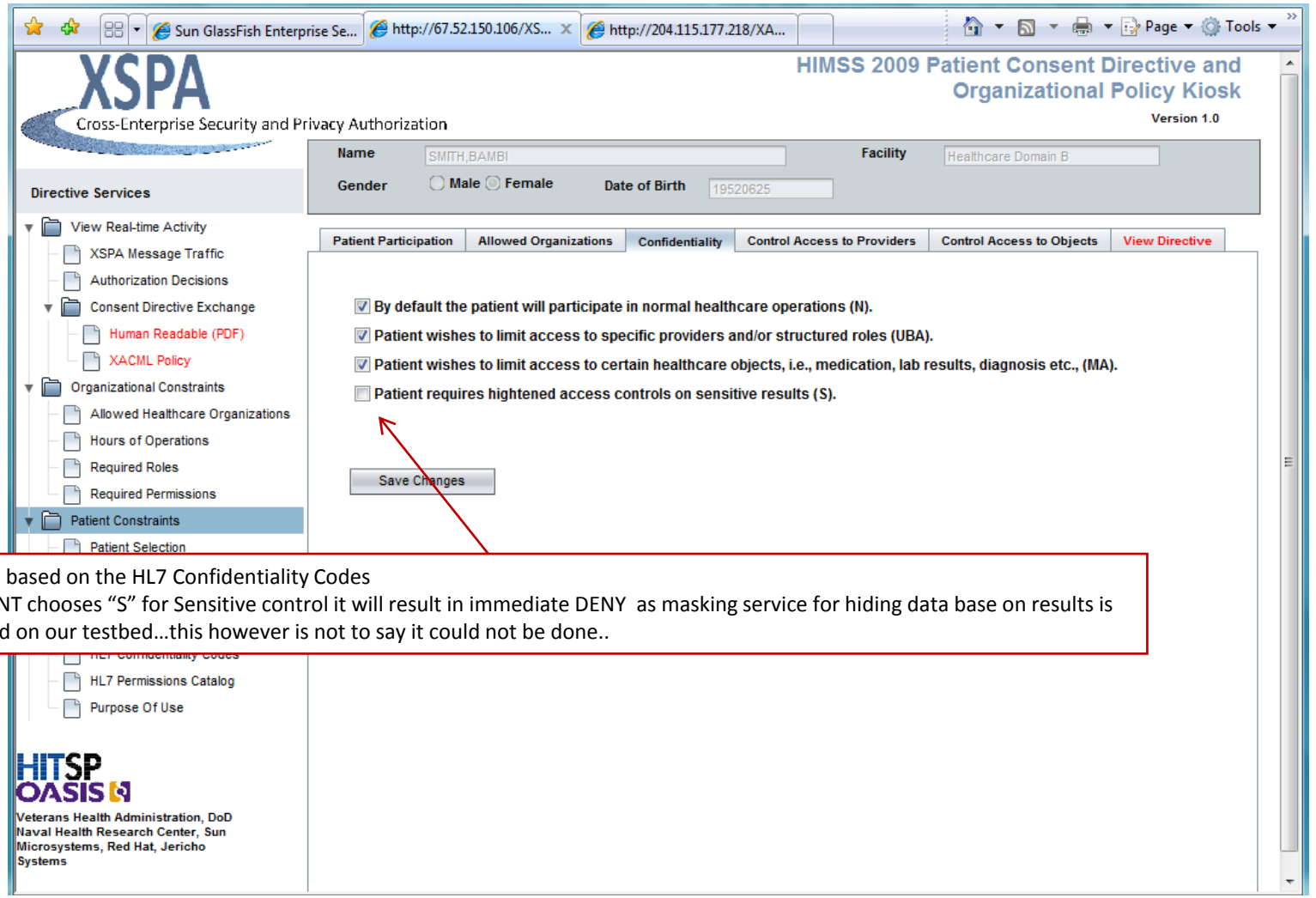


Patient Consent Directive



Patient can limit access based on requesting organization, only organizations Domain B that have been setup at the in “Organizational Constraints” are available to patient.

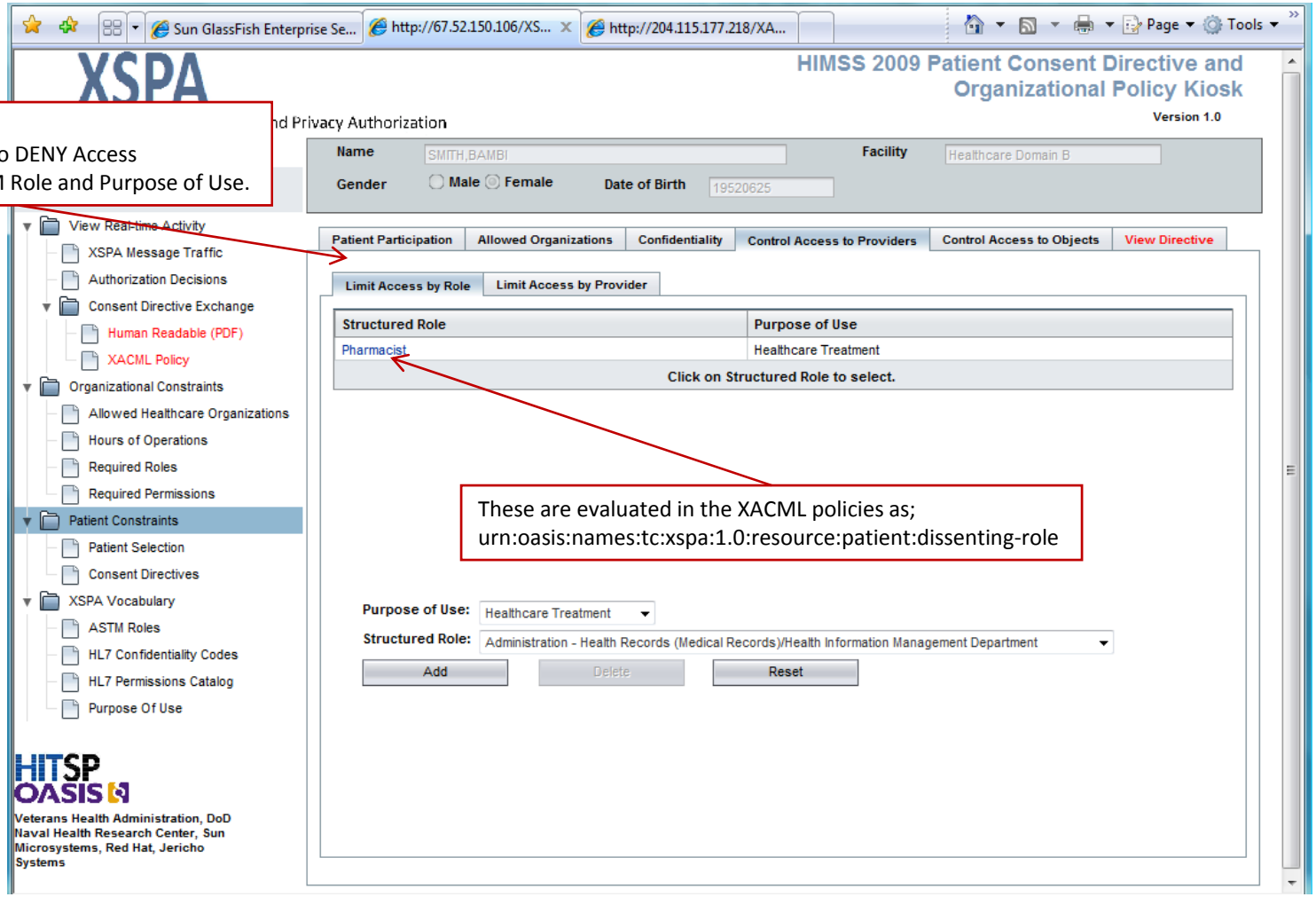
Patient Consent Directive



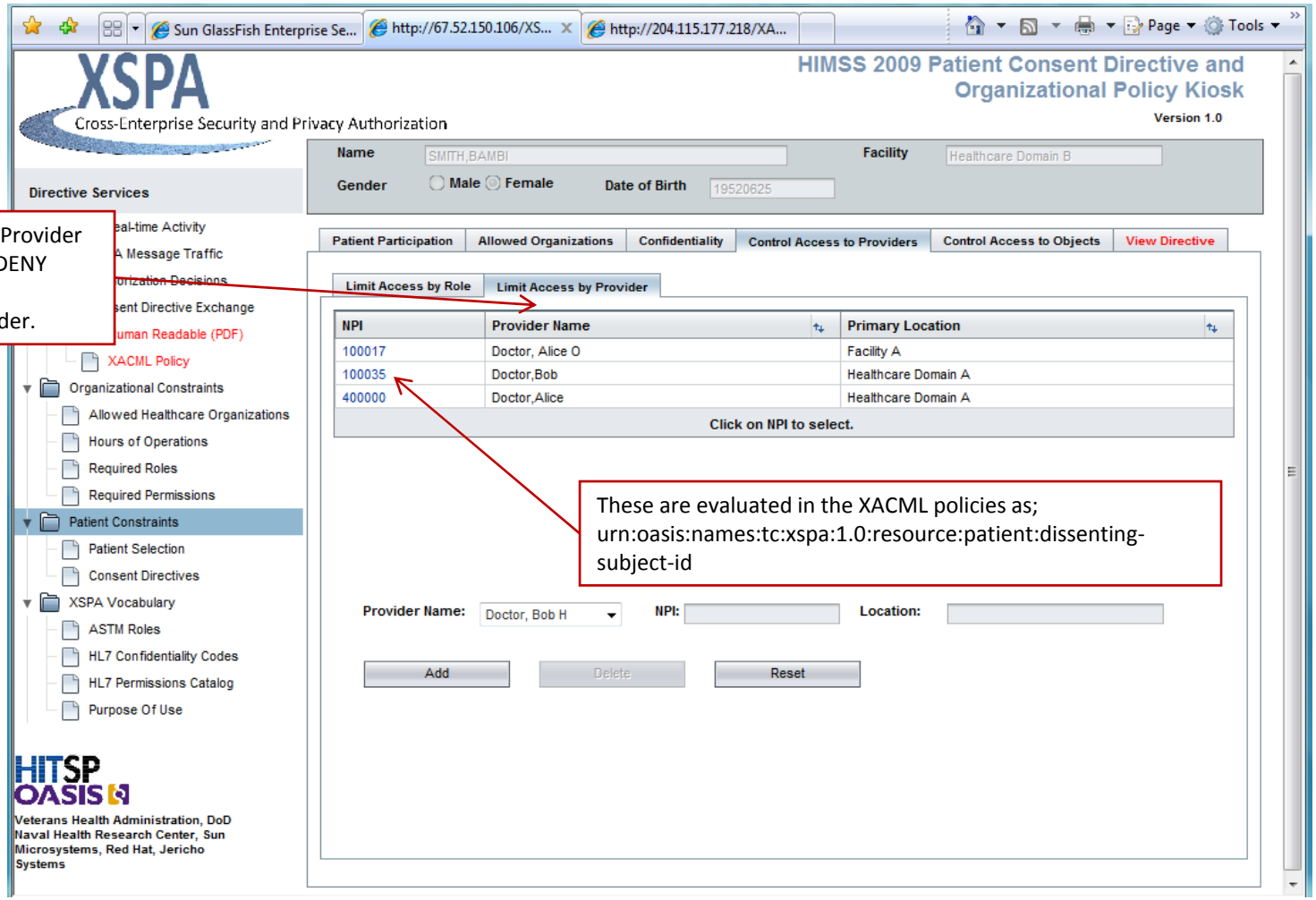
Confidentiality is based on the HL7 Confidentiality Codes
NOTE: If a PATIENT chooses "S" for Sensitive control it will result in immediate DENY as masking service for hiding data base on results is Not implemented on our testbed…this however is not to say it could not be done..

Patient Consent Directive – UBA Constraint Based on Role and Purpose of Use

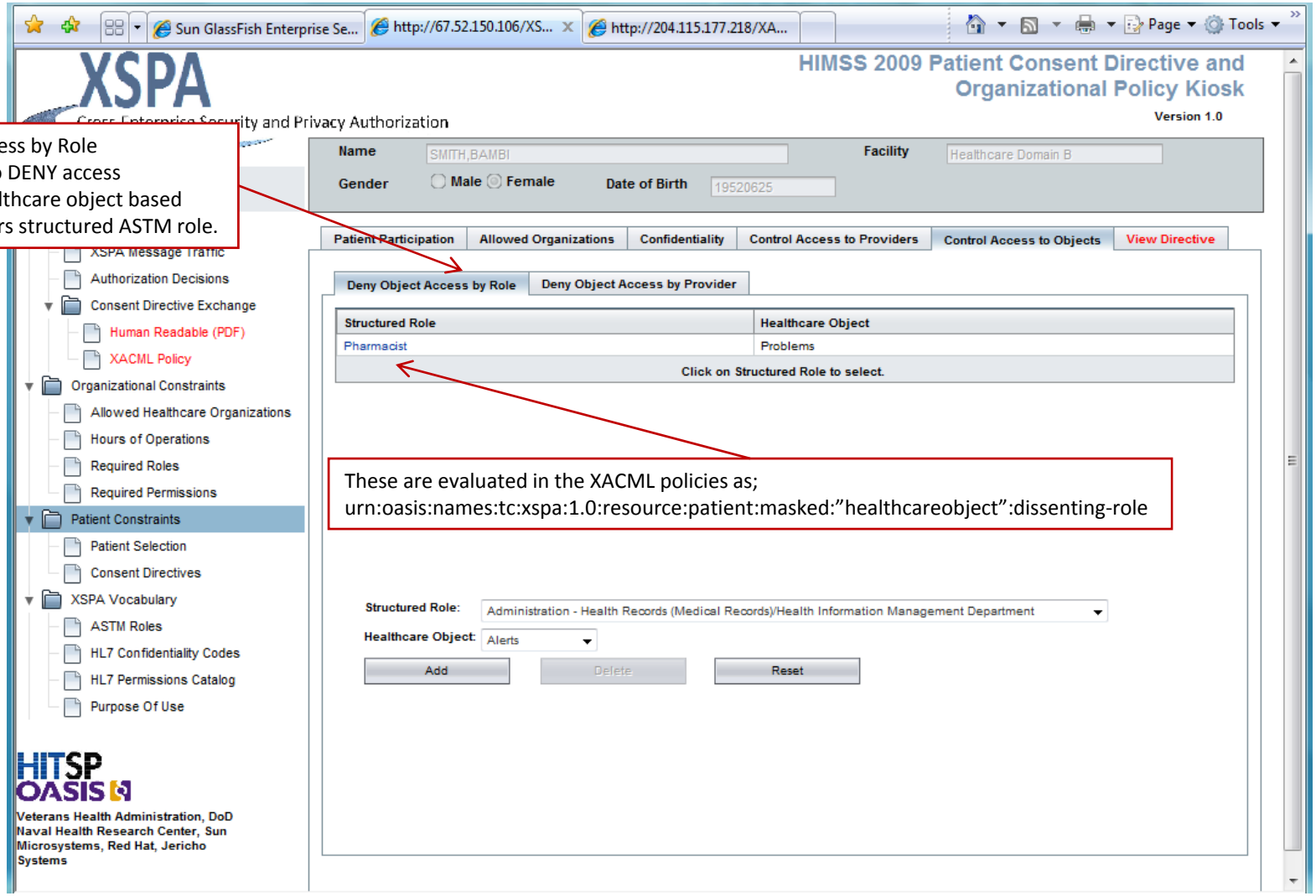
Limit Access by Role
Allows patient ability to DENY Access
Based on a users ASTM Role and Purpose of Use.



Patient Consent Directive – UBA Constraint Based on a Specific Provider



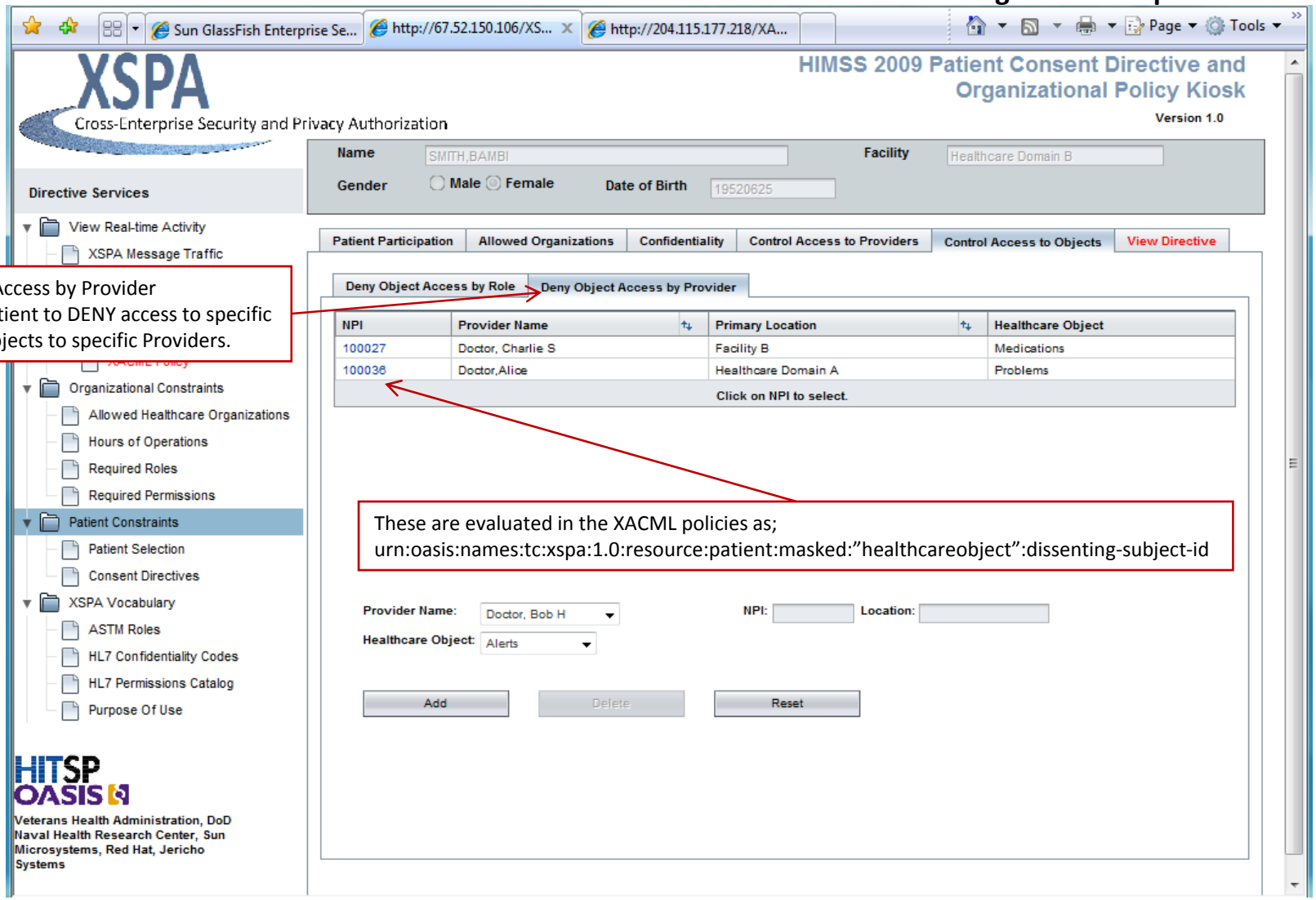
Patient Consent Directive – MA Constraint
Masking Based on Role



Deny Object Access by Role
Allows patient to DENY access
To a specific healthcare object based
On the requestors structured ASTM role.

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

Patient Consent Directive – MA Constraint
Masking Based on Specific Provider

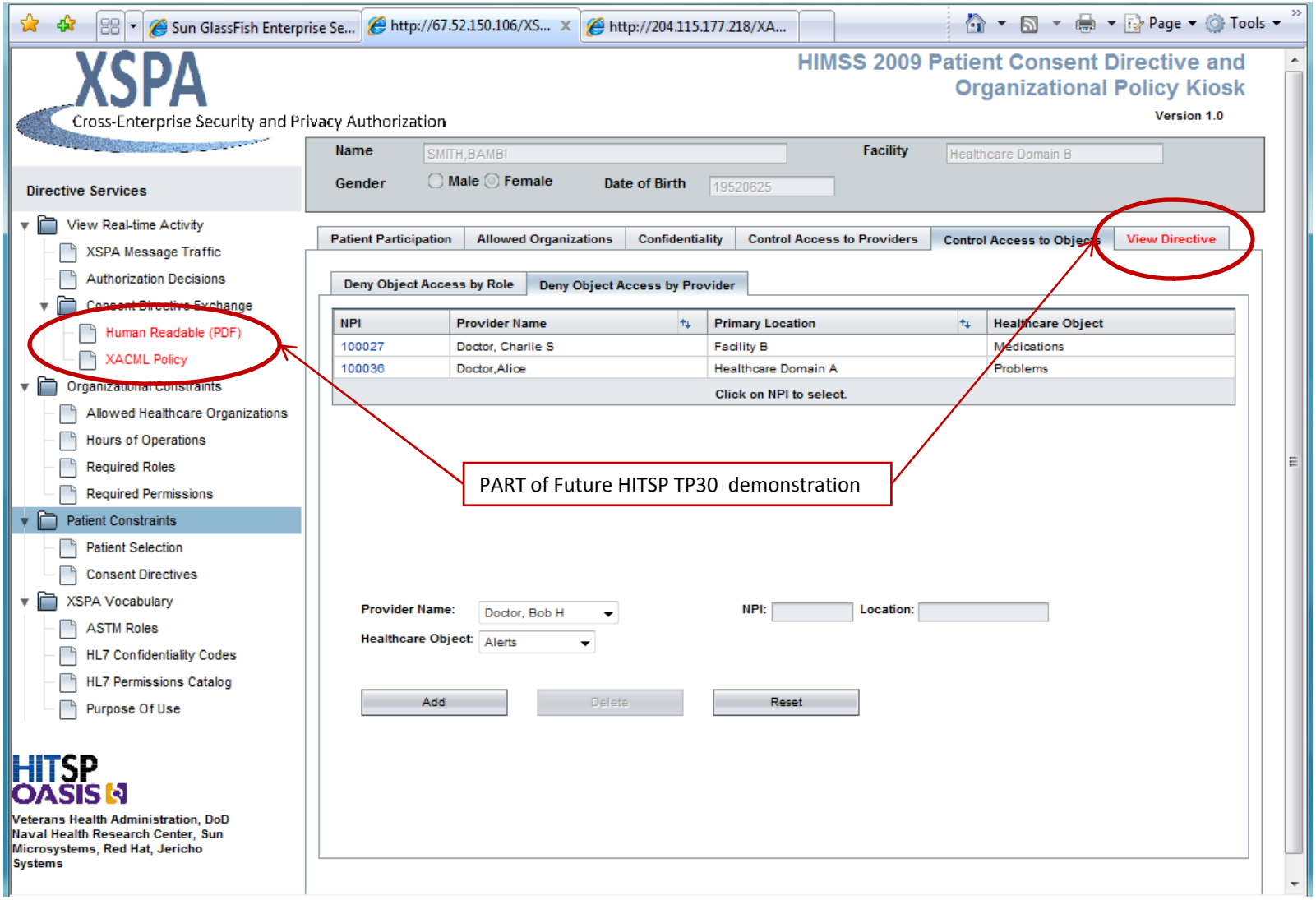


Deny Object Access by Provider
Allows the patient to DENY access to specific Healthcare objects to specific Providers.

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

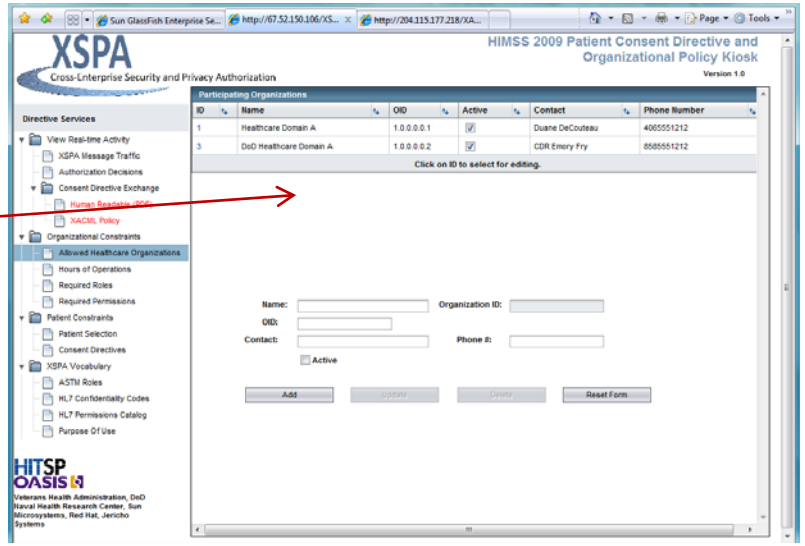
HIMSS Patient Privacy and Access Control Advanced Technology Demonstration

Patient Consent Directive – TP30
Viewing Directive

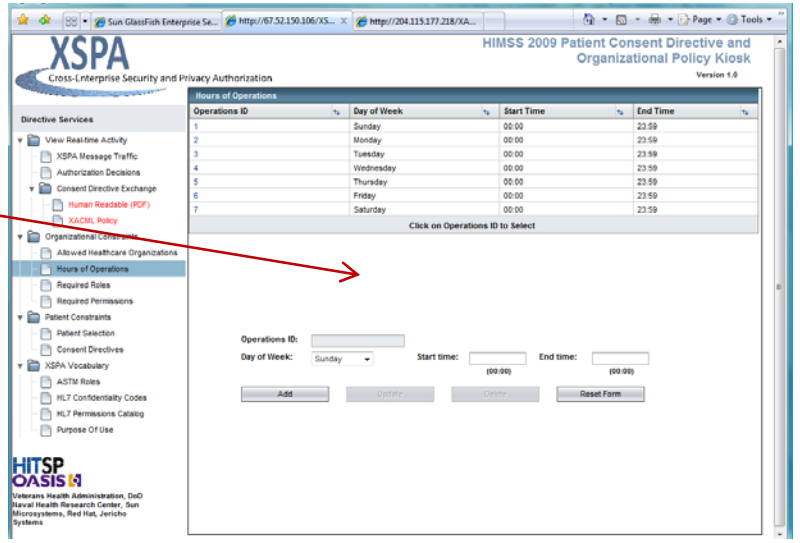


Organizational Constraints

Allowed Organizations
Provides control over which participating organizations.
This is evaluated in the XACML policies as;
urn:oasis:names:tc:xspa:1.0:resource:org:allowed-organizations



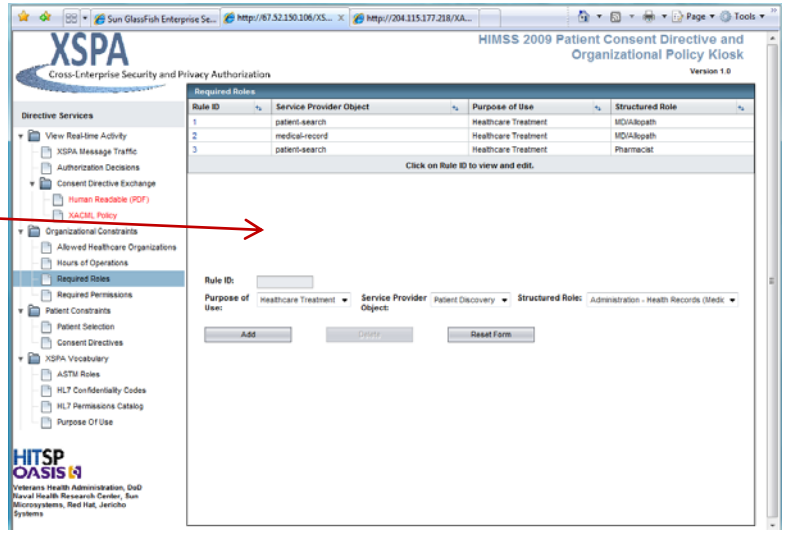
Hours of Operation
Provides control over when services are available
This is evaluated in the XACML policies as;
urn:oasis:names:tc:xspa:1.0:resource:org:hoursofoperation:start
urn:oasis:names:tc:xspa:1.0:resource:org:hoursofoperation:end



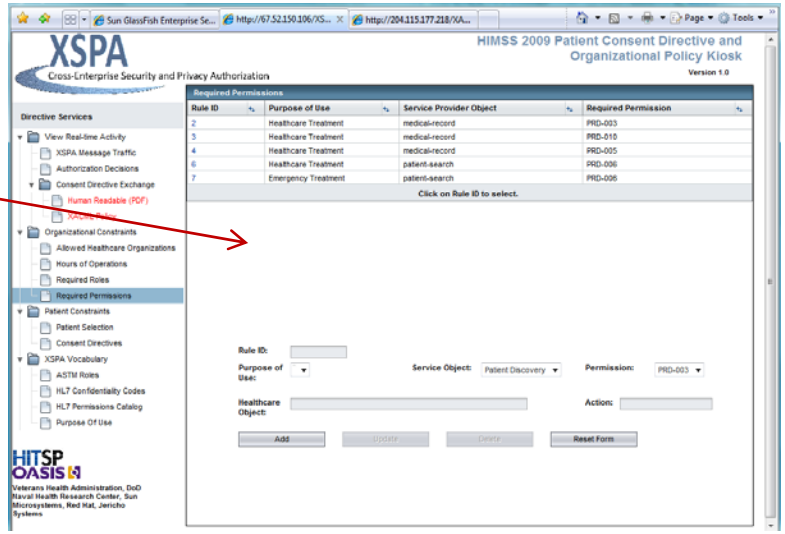
HIMSS Patient Privacy and Access Control Advanced Technology Demonstration

Organizational Constraints

Required Roles
Allows organization to control who has access to specific Services based on their structured role and purpose of use. These are evaluated in the XACML policies as;
urn:oasis:names:tc:xspa:1.0:resource:org:role



Required Permissions
Allows organization to set required permissions for a specific service. These are evaluated in the XACML policies as;
urn:oasis:names:tc:xspa:1.0:resource:org:hl7:permission



Viewing Clinical Summary

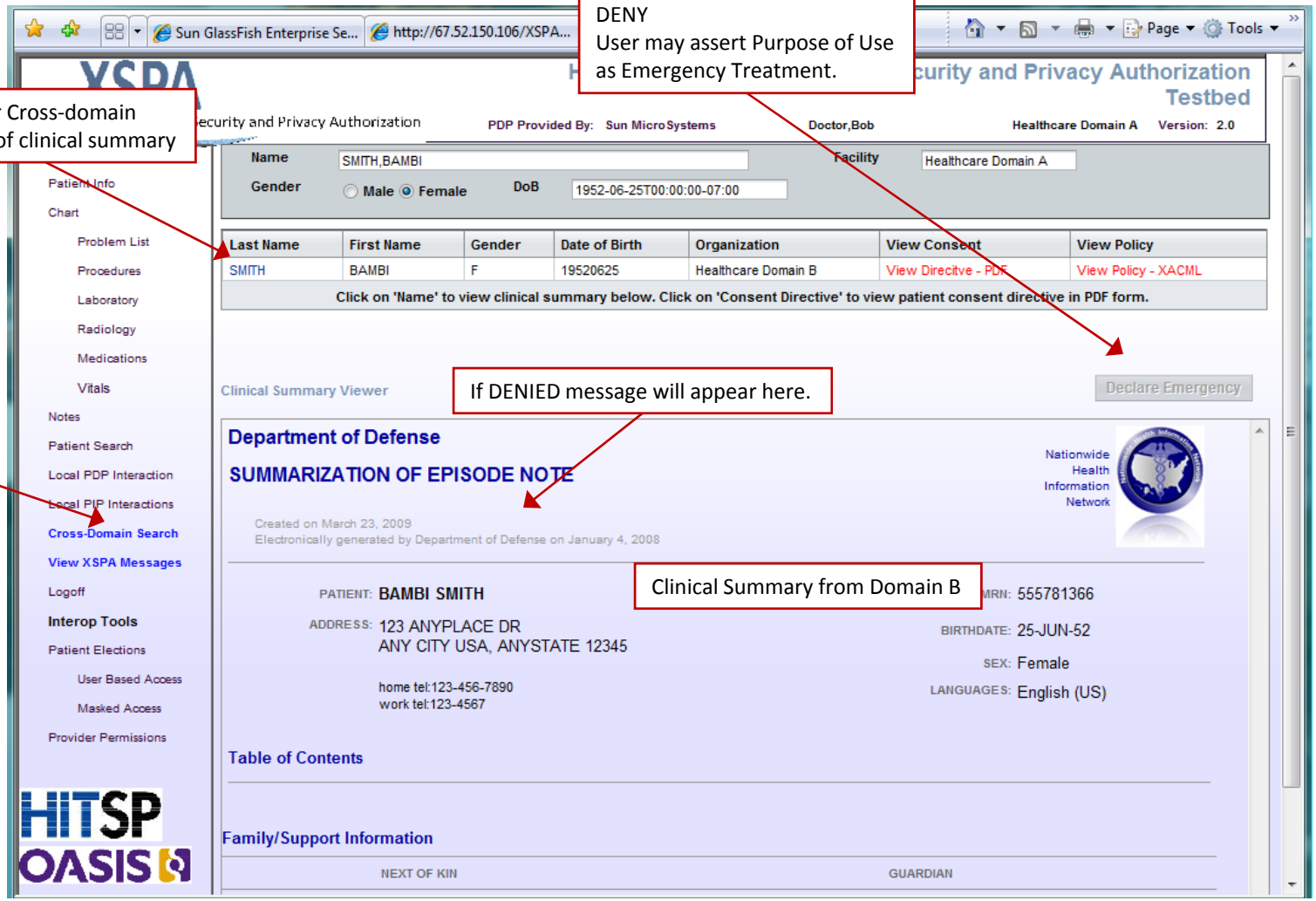
In access control decision is DENY
User may assert Purpose of Use as Emergency Treatment.

Select for Cross-domain Request of clinical summary

Select to Perform Cross-domain patient discovery

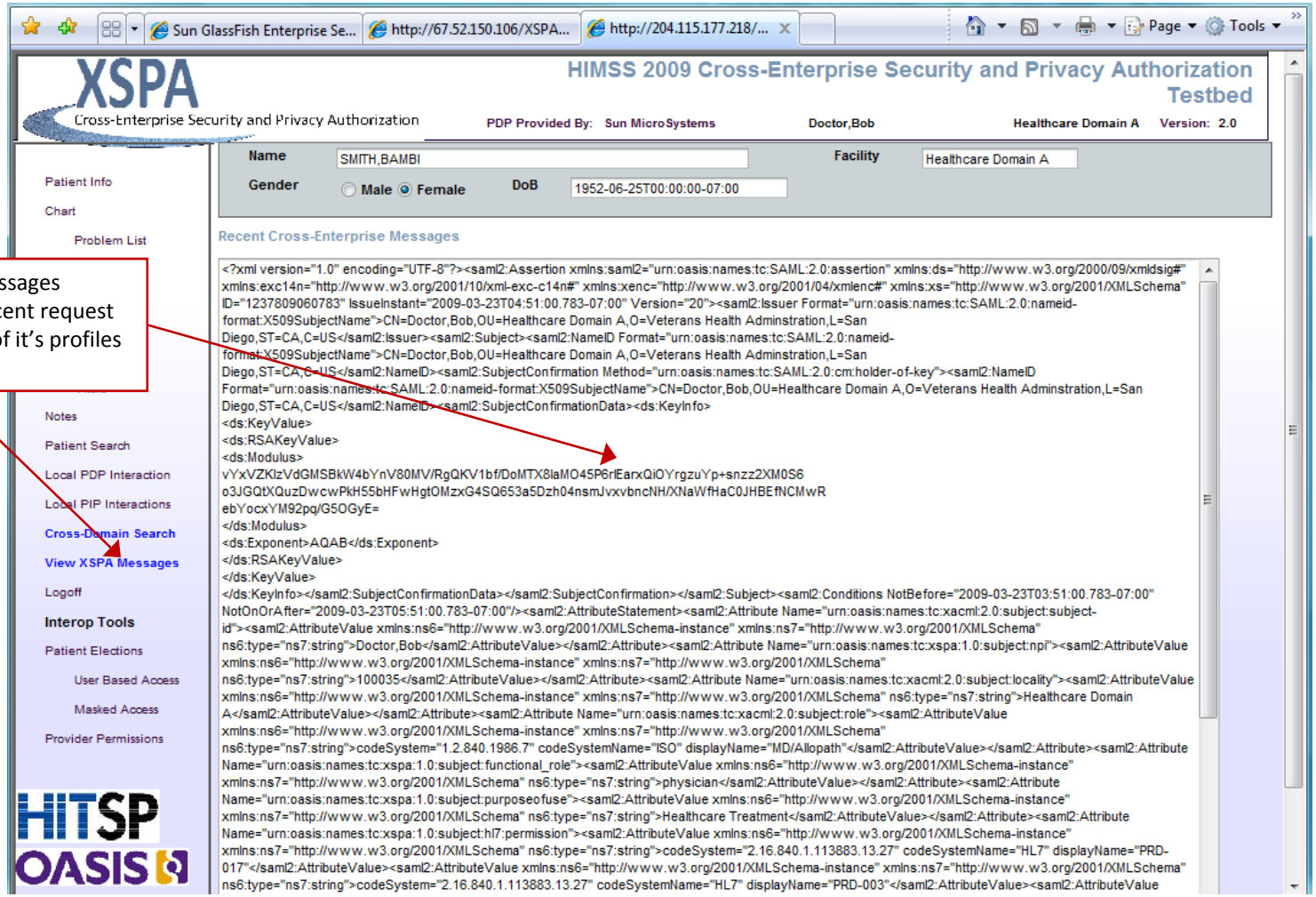
If DENIED message will appear here.

Clinical Summary from Domain B



Viewing XSPA Request

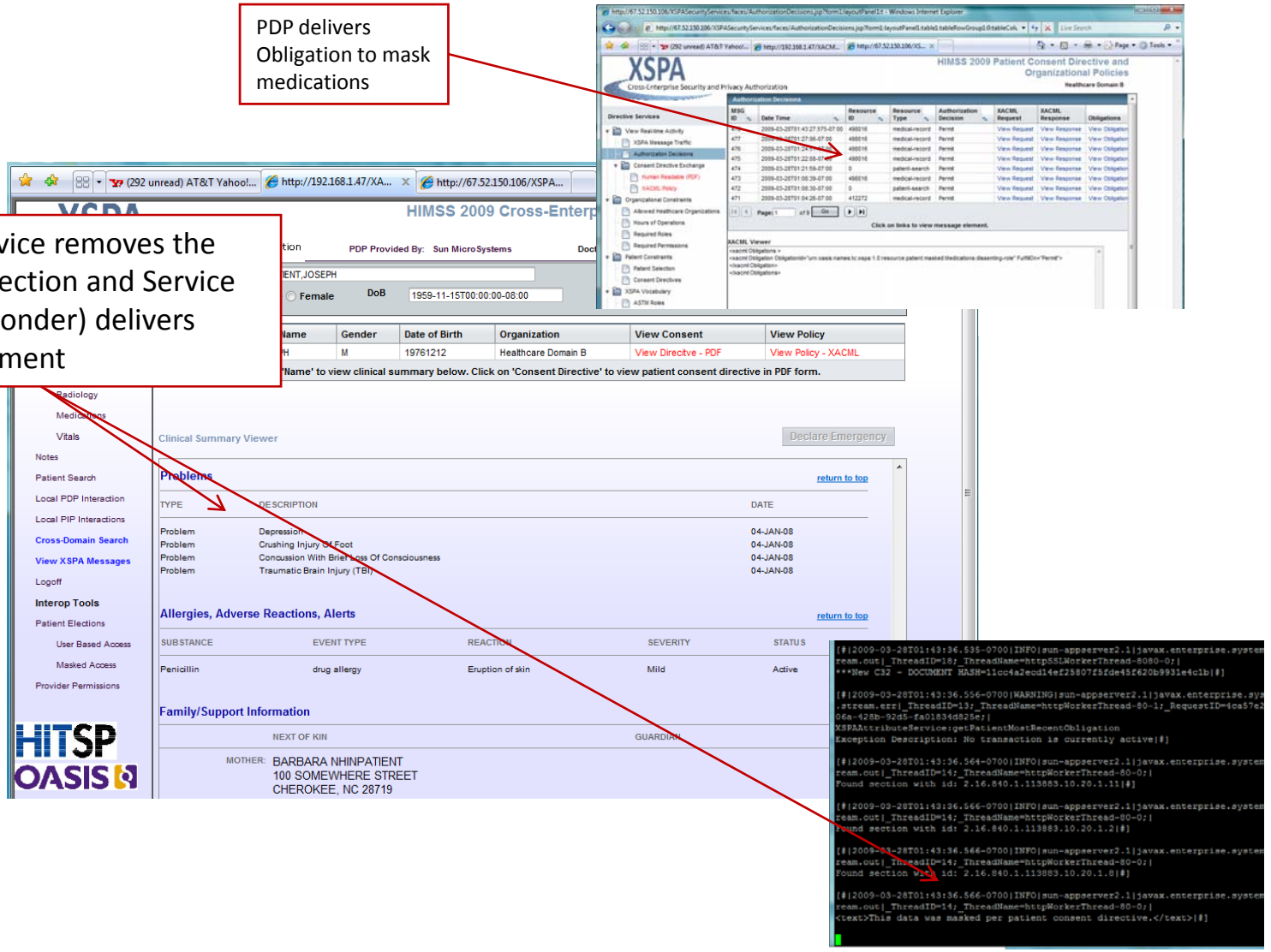
Selecting View XSPA Messages
Will display the most recent request
Including the assertion of it's profiles
Attributes.



Example Interaction Between Domains

PDP delivers Obligation to mask medications

Redaction service removes the Medications section and Service Provider (responder) delivers updated document



USE CASE #1 EXAMPLE

In this example, the Domain B patient privacy policy restricts access so that Dr. Bob (by name or role) cannot see meds report information for patient "X" even though he is asserting authorizations granted by Domain A.

USE CASE #1 EXAMPLE PRECURSORS

- Partners establish trust relationships between organizations
- Information owner establishes data access policies
- Patient makes policy preferences known (consent directives)(POU, UBA, MA)
- Policy and attribute stores are provisioned

USE CASE #1 EXAMPLE Requestor (Domain A)

- Clinician searches for patient
- Submits a request
  - Includes authorizations
  - Includes credentials
- Receives Data

USE CASE #1 EXAMPLE Responder (Domain B)

- Receive request+Authn+Authz
- Determine POU and applicable policy set
- Return the response masked based on patient consent directive
- We sill see the request granted.

USE CASE #2 EXAMPLE Emergency

In this example, the Domain B patient changes their privacy policy to deny all Nurses access to their medical record. Nurse Charley cannot see the patient's record even though he is asserting authorizations granted by Domain A. Nurse Charley asserts a medical emergency from Domain A and subsequently is able to see the patient's record from Domain B.

USE CASE #2 EXAMPLE Precursors

- Partners establish trust relationships between organizations
- Information owner establishes data access policies
- Patient makes policy preferences known (consent directives)(POU, UBA)
- Policy and attribute stores are provisioned

USE CASE #2 EXAMPLE Requestor

- Clinician searches for patient
- Submits a request
  - Includes authorizations
  - Includes credentials
- Receives Data
- Declares an Emergency
- Receives Data

USE CASE #2 EXAMPLE Responder

- Receive request+Authn+Authz
- Determine POU and applicable policy set
- Return the response masked based on patient consent directive
- We sill see the request granted
  - POU normal: no access to nurses in domain A
  - POU emergency: allow access to nurses in domain A