Using Service Aware Standards to Secure the Exchange of the Electronic Health Record

SOA in Healthcare Conference

Arlington, VA

John (Mike) Davis
David Staggs (SAIC)
Department of Veterans Affairs

July 12, 2010
On April 9, 2009, President Obama directed the Department of Defense and the Department of Veterans Affairs to create the Virtual Lifetime Electronic Record:

“... will ultimately contain administrative and medical information from the day an individual enters military service throughout their military career and after they leave the military.”

-President Barack Obama
Virtual Lifetime Electronic Record Strategy

- Allow health care providers access to Servicemembers’ and Veterans’ health records, in a secure and authorized way, regardless of whether care is delivered in the private sector, Department of Defense (DoD), or VA
- More efficient, effective, and timely than creating a single DoD /VA system
  - Builds on existing DoD and VA Electronic Health Record capabilities
  - Solves the need to share information with the private sector
  - Not a large acquisition program
  - Avoids obsolescence as Electronic Health Record systems modernize
Top Health Care System Security Requirements

- Security and privacy infrastructure for end-to-end data sharing
- High-assurance person identifiers across federated domains
- Organizational and personal policy enforcement
- User accountability for potential security events (audit)
- Security assurance, interoperability through standards, common processes, and system certification
Key Concept: Enforce both Consumer and Enterprise Privacy policy with Common Security Services

- Enforcing consumer privacy policy is a security concern
- Agreement to enforce privacy is a business decision/contract with consumer
- Basic consumer privacy policies both control access and constrain security
Web of Standards and Related Organizations

- HL7
  - CDA Consent Directive
  - Health Care Functional Role Standard
  - SOA Security and Privacy
  - Security/Privacy Info Models
  - Privacy Confidentiality Codes
  - HL7 Service Aware Architecture

- ISO via US TAG
  - Privilege Management
  - Structural and Functional Roles, +++

- NHIN
  - NHIN Updates

- OASIS
  - SAML, XACML, WS-Trust Profiles

- CCHIT
  - Certification Profiles

- IHE
  - Health Care Profiles

- ASTM
  - Privilege Management
  - Structural Roles

- HITSP
  - Authorization/Privacy Preference standards and Interface Specifications

- ANSI-INCITS
  - RBAC Standard
  - RBAC Implementation

- NIST
  - FIPS/Special Publications

- Demos

Text Color Key:
- Standards
- Models/Draft standards

- CDA=Clinical Document Architecture
- FIPS=Federal Information Processing Standard
- HL7=Health Level 7
- HITSP=Healthcare Information Technology Standards Panel
- NHIN=Nationwide Health Information Network
- ISO=International Standards Organization
- NIST=National Institute of Standards & Technology
- OASIS=Organization for the Advancement of Structured Information Standards
- RBAC=Role Based Access Control
- SAML=Security Assertion Markup Language
- SOA=Service Oriented Architecture
- XACML=Extensible Access Control Markup Language

Veterans Health Administration | Office of Health Information
Key Concept: Validate approach through interoperability demonstrations (reference implementations and testing)

- **RSA Conference March 2010** – Multi-vendor demonstration of NHIN Connect Security & Privacy
- **HIMSS Apr 2009** – First end-to-end demonstration of privacy consents and access control
- **London Conference Oct 2008** – Extensions to the RSA demonstration adding SAML
- **RSA Conference April 2008** – Multi-vendor demonstration of OASIS XACML profile

- **Clinical Roles and Permissions**: Clinician least privilege
- **Emergency Access**: Granting extraordinary access during events involving risk of potential death or injury
- **Patient Consent Directives**: Patient driven authorizations to personal health information use and disclosure
- **Healthcare Security Policy**: Healthcare specific business rules for application behavior and patient safety

**Abbreviations**

- HIS = Health Information System
- NHIN = Nationwide Health Information Network
- SAML = Security Assertion Markup Language
- XACML = eXtensible Access Control Markup Language
Implementation
Reference Model Overview

GW = Gateway
PEP = Policy Enforcement Point
ROI = Release of Information Office
Consumer Privacy & eConsent
Meet ONC Consumer Preferences Requirements

Consumers should be able to:

- Define permissions for who is permitted to access information
- Express how their health information would be made available
- Authorize release of their health information
- Establish various types of consumer preferences (consents, advance directives, etc.)

Define privacy preference conditions including:

- By type of information (all data, segmentation of data)
- By role and criteria based access, including type of encounter, embargoed records (VIP, legal restrictions)
- By time (start, end, duration)
- By level of participation (opt-in, opt-out, with or without additional classifications, with or without additional granularity)
- By purpose of use

NHIN=Nationwide Health Information Network
ONC=Office of the National Coordinator
VIP=Very Important Person
Patient Viewpoint (to-be)

Consent Directive
eConsent Signature Service Framework

1. Authentication Service
2. Demographic Service
3. User Input
4. Electronic Forms Service
5. Signature Service
6. Approval
7. Electronic Forms Repository
8. Signature Service
9. Electronic Forms Repository

Veteran Patient

User Input

Signature is bound to document

Electronic Forms Service

Approval

Electronic Documents Repository
Leverages HL7 Consent Directive Analysis Model
Privacy Management
### Patient Details

**Opt in/Out**

#### Patient Demographics
- **SSN**: 888800001
- **ICN**: 1012581678v377002
- **Name**: CHDRZZTESTPATIENT, CHDRONIE
- **Gender**: M
- **Date of Birth**: 03/03/1980
- **Marital Status**: M
- **Address**: 1234 Howard St, LA JOLLA, CA 92038
- **Multiple Birth**: NO
- **Phone #**: tel:(760)222-5555

#### Patient is Opted In

The patient's data is being shared with other providers on the NHIN. Click Opt Out to disable sharing of this patient's data. **NOTE:** A patient's Opt In/Out status does not affect interactions with the Department of Defense (DoD). VA patient information is always shared with the DoD.

- **Opted In**: 06/10/2010
- **Expires**: 06/09/2014
- **Reason for Opt Out**: --Select a reason--

#### NHIN Correlations

<table>
<thead>
<tr>
<th>FACILITY NUMBER</th>
<th>PROVIDER NAME</th>
<th>PATIENT ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>200NHKP</td>
<td>blah</td>
<td>679206</td>
</tr>
</tbody>
</table>

**Remove Correlations**

Remove correlations to NHIN partners from VA's Master Patient Index. Correlations to DoD will not be removed.

**Announce/Revoke**

Announce a patient to the NHIN. If the patient is not Opted In, he/she will only be correlated with providers where the patient is known and no Opt In is required (e.g., DoD).

- **Announce**: Broadcast this patient's demographics to the NHIN to create correlations with other providers at which the patient is known.
Security Management
Security Management

- Provide control and management of security mechanisms providing security services
- Control and provision enterprise security policy, identity and authorizations (IAM) and other security information
- Generate configuration data, cryptographic keys
- Provide security management for logging of security relevant events, recovery and support for breach reporting
VA Identity and Access Management

Identity Proofing – Standardized Proofing Process

- **Veterans**
- **Beneficiaries**
- **Employees**
- **Contractors**
- **Affiliates**

**VA Trusted Agent**

**Administer Identity**
- **Check Identity**
- **Verify & Capture Identity**
- **Provide Identity Information**

**Correlate & Store**

**Proofing Repository**

**Proofing Service Provider**

**Other Sources (SSA, OPM, etc.)**

**Virtual Directory Server**

**Identity Proofing Process**

**VIC Card Issuance Process**

**E-Auth Credentialing Process**

**PIV Card Process**

**Veterans & Beneficiaries**

**Employees, Contractors, & Affiliates**

**BIRLS**=Beneficiary Identification and Records Locator System
**eBenefits**=Electronic Benefits
**ETA/IFCAP**=Integrated Funds Control, Accounting, and Procurement
**LMS**=Learning Management System
**MPI**=Master Patient Index
**PAID**=Personal and Accounting Integrated Data System
**PIV**=Personal Identity Verification
**VADIR**=VA/DoD Identity Repository
**VISTA**=Veterans Health Information Systems and Technology Architecture
Access Control Service
Consumer Preferences and Policy (CPP) SOA High-Level Framework

HITSP TP20 Access Control, TP30 Manage Consent Directives, OASIS XSPA SAML, WS-TRUST

HITSP=Healthcare Information Technology Standards Panel
OASIS=Organization for the Advancement of Structured Information Standards
SAML=Security Assertion Markup Language
TP=Transaction Package
XACML=Extensible Access Control Markup Language
HL7 Access Control Service Framework
Attributes use to enforce security and privacy in an XSPA cross-enterprise exchange of patient data

- **SubjectID (User)**
  - Unique identifier specific to a given entity.

- **Purpose of Use (POU)**
  - Described in XSPA profiles and mutually agreed upon by participating entities.

- **Role (S)**
  - Structural Role
  - Refer to [ASTM E1986-98 (2005)]

- **Role (F)**
  - Functional Role
  - Refer to ANSI-INCITS 359-2004 Compliant [HL7-PERM]

- **Location**

- **Organization**

- **Permission 1 {Action, Object}**
- **Permission 2 {Action, Object}**
- **Permission 3 {Action, Object}**
- **Permission …N {Action, Object}**
NHIN San Diego Physical Deployment (To-Be)

ADI = Access Control Decision Information
CDS = Clinical Data Services
HDR = Health Data Repository
MPI = Master Patient Index
NHIN = Nationwide Health Information Network
PDP = Policy Decision Point
PEP = Policy Enforcement Point
ROI = Release of Information
RPC = Remote Procedure Call
WS = Web Services
XACML = eXtensible Access Control Markup Language
Advanced Concept Demonstrations

Protecting the Human Genome - RSA 2010

PHR Service
Patient has ability to view their Genotype and determine whether to deny access to all or portions of it.

XSPA Enabled Service Provider

Access Control System

Patient Policy
Constrains access to specific AT-RISK SNPs based on characteristics and/or disease grouping

Constraints

PIP

PDP

PEP

Assertion Consumption

Clinical Adaptive Services

Request for Patients genotype

Response

Provider

Continuous Re-validation of Patient Policy Intent

Original Mapping

Patient's Genotype

New diseases and characteristics are mapped

Multiple Organizations Contribute Findings

Trusted/Clinically relevant providers

GWAS=Genome-wide Association Study
PDP=Policy Decision Point
PEP=Policy Enforcement Point
PHR=Patient Health Record
PIP=Policy Information Point
SNIP=Single Nucleotide Polymorphism
XSPA=Cross-enterprise Security and Privacy Authorization

Veterans Health Administration | Office of Health Information
System and Participant Locations
- RSA 2008 – San Francisco, CA
- Oasis XACML InterOp Demonstration – Ditton Manor, London, UK
- HIMSS 2009 – Chicago, IL
- RSA 2010 – San Francisco, CA
Implemented Security and Privacy Policies

- **Demonstrate the Enforcement of Patient Consent Directives**
  - Opt-In / Opt-Out
  - Deny Access based on Organizations
  - Deny Access based on Role
  - Deny Access based on Purpose of Use*
  - Deny Access to Specific Providers
  - Mask C32 Results based on Role (future release)**
  - Mask C32 Results for Specific Providers (future release)**
  - Mask C32 Results based on data sensitivity (not supported)

- **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

  * Demonstration only. Current model is single purpose of use
  **Future capability. Requires ability of Adaptor to accept obligation
Denial based on subjects ASTM structured role:
**View of Summary of Care Record (C32)**

### Kaiser Permanente

**Summarization of episode note**

It is important to understand that not all of the patient's current conditions may be listed in the Problem List. Certain conditions such as, but not limited to, behavioral health and substance abuse diagnoses are not included in the Problem List due to filtering. Based on these limitations you should not rely on the Problem List as the sole source for determining the existence or non-existence of a patient condition. Diagnoses will be displayed in other portions of the record.

**Created On:** January 4, 2010

**Patient:** CHORB6THREE CDRZ7ZTESTPATIENT

1421 HOWARD ST.

LA JOLLA, CA 92038

Tel: 1-858-888-3452 Home

**Birthday:** March 3, 1962

**Language(s):** English

**Source:** Kaiser Permanente

**Patient ID:** 000013757744

**Sex:** M

### Problems

<table>
<thead>
<tr>
<th>Problems</th>
<th>Problem Code</th>
<th>Date</th>
<th>Provider</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acquired Immunodeficiency Syndrome</td>
<td>--</td>
<td>Dec 16, 09</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Acute Peptic Ulcer, Perforated</td>
<td>--</td>
<td>Dec 16, 09</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hypertension</td>
<td>--</td>
<td>Nov 14, 09</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Diabetes Mellitus, Type 2, Uncontrolled</td>
<td>--</td>
<td>Feb 14, 08</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Diabetes Mellitus, Type 2, Uncontrolled</td>
<td>--</td>
<td>Nov 29, 07</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Abdominal Pain, Chronic</td>
<td>--</td>
<td>Oct 23, 06</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Allergies, Adverse Reactions, Alerts

<table>
<thead>
<tr>
<th>Allergens</th>
<th>Event Type</th>
<th>Reaction Type</th>
<th>Severity</th>
<th>Verification Date</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>BANANA</td>
<td>--</td>
<td>Headaches</td>
<td>--</td>
<td>Nov 14, 09</td>
<td>--</td>
</tr>
<tr>
<td>ACETAMINOPHEN-CODEINE</td>
<td>--</td>
<td>Skin Rash and/or Hives</td>
<td>--</td>
<td>Dec 16, 09</td>
<td>--</td>
</tr>
</tbody>
</table>

### Medications

<table>
<thead>
<tr>
<th>Medications</th>
<th>Brand Name</th>
<th>Route</th>
<th>Interval</th>
<th>Status</th>
<th>Prescription NBR</th>
<th>Dispense Date</th>
<th>Provider</th>
<th>Quantity (SL)</th>
<th>Order Expired</th>
</tr>
</thead>
<tbody>
<tr>
<td>LISINOPRIL 40 MG ORA</td>
<td>LISINOPRIL 40 MG ORAL TAB</td>
<td>--</td>
<td>--</td>
<td>Active</td>
<td>--</td>
<td>--</td>
<td>WILLIAM EDWIN BO</td>
<td>--</td>
<td>Nov 14</td>
</tr>
<tr>
<td>IMIQUIMOD 5 % TOP F.</td>
<td>IMIQUIMOD 5 % TOP PACK</td>
<td>--</td>
<td>--</td>
<td>Active</td>
<td>--</td>
<td>--</td>
<td>WILLIAM EDWIN BO</td>
<td>--</td>
<td>Sep 23</td>
</tr>
<tr>
<td>AMOXICILLIN 500 MG</td>
<td>AMOXICILLIN 500 MG ORAL CAP</td>
<td>--</td>
<td>--</td>
<td>Active</td>
<td>--</td>
<td>--</td>
<td>WILLIAM EDWIN BO</td>
<td>--</td>
<td>May 21</td>
</tr>
</tbody>
</table>
Current State

- Nationwide Health Information Network Connect provides a basic Policy Decision Point (PDP)
  - Jericho Systems PDP with 12 pre-filled policies
  - Used in interoperability demonstrations

- Can be used to deploy, test, and benchmark any provider’s solution
Next Steps

- OASIS Reference Model
- XSPA Profile of WS-Trust
- OASIS XACML Ontology
- OASIS Privacy Management Reference Model (PMRM)
- HL7 SOA PASS Audit
- HL7 Security and Privacy Ontology
- HL7 Services Aware Interoperability Framework
- ISO Purpose of Use
Summary

- Core service aware standards are in place and new standards are under development
- Domain information models customize the services specification to accommodate individual verticals
- Vendors have demonstrated the ability to implement security and privacy services protecting electronic health records
- Clinical adaptive services can extend the reach of security to protect segmented data in the electronic health record
For Further Information
Demonstration Videos

Use Case Examples
Patient Privacy – Clinical Data Masking
Healthcare Organization Policy – Emergency Treatment
Protecting the Human Genome

Overviews
XSPA Technology Overview – Part 1
XSPA Technology Overview – Part 2a
XSPA Technology Overview – Part 2b

http://www.youtube.com/watch?v=RKbAtmgWGz4
http://www.youtube.com/watch?v=8aA2Uy6lsQs
http://www.youtube.com/watch?v=A3HtXCu2sa8

*Larger videos are available for viewing at: http://www.ascendahealthcare.com/himss2009.html
Nationwide Health Information Network: San Diego Project

**News Report**

- Electronic processes replace paper-based health information requests saving weeks or months
- Advanced security and privacy mechanisms ensure appropriate access to patient records
- Patients have the option to allow or prevent sharing of some of their information