The Standards and Interoperability (S&I) Framework

in cooperation with

Health Level Seven (HL7)

Presents

Data Segmentation for Privacy

Disclaimer: This Pilot demonstration does not represent the official position or policies of the ONC, the Substance Abuse and Mental Health Services Administration, or the Department of Veterans Affairs. This Pilot demonstration is for educational purposes only and does not constitute legal advice or opinion.
Data Segmentation for Privacy Pilot

The Standards and Interoperability (S&I) Framework in collaboration with Health Level Seven (HL7)
presents a Privacy Pilot for sending and receiving health information protected by metadata classification “tags” indicating confidentiality, sensitivity, and handling instructions.

John has enrolled in an alcohol and drug abuse treatment program. He is embarrassed but knows he needs help. His primary care physician (PCP) is someone he trusts and he wants to share his treatment information because of related problems. He signs an authorization allowing sharing of his alcohol treatment information with his PCP. He is advised that his PCP cannot further re-disclose information about his alcohol treatment without his authorization, which was a concern. John’s Summary of Care record is automatically coded or “tagged”, providing the means to provide the special handling needed. Some time later, John’s PCP wants to send John’s “segmented” information to a specialist. Document tagging allows the PCP system to intercept this unauthorized re-disclosure.
What is the S&I Framework?

The S&I Framework is a collaborative community of volunteers from the public and private sectors who are focused on providing the tools, services and guidance to facilitate the functional exchange of health information.

The S&I Framework uses a set of integrated functions, processes, and tools that enable execution of specific value-creating initiatives. Each S&I initiative tackles a critical interoperability challenge through a rigorous process that typically includes:

- Development of clinically-oriented user stories and robust use cases
- Harmonization of interoperability specifications and implementation guidance
- Provision of real-world experience and implementer support through new initiatives, workgroups and pilot projects
- Mechanisms for feedback and testing of implementations, often in conjunction with ONC partners such as NIST

ONC=Office of the National Coordinator
NIST=National Institute of Standards and Technology
What is Data Segmentation of Health Care Information?

• The term “Data Segmentation” refers to the process of sequestering from capture, access, or view personal health information that is perceived by a legal entity or individual as being undesirable to share.

• This basic definition, however, does not account for the multiple permutations of segmentation in the health care context (i.e., granularity) nor does it adequately capture the varied considerations required for development of segmentation policy.
What is the S&I Data Segmentation for Privacy (DS4P) Initiative?

**Challenge:** Enable the implementation and management of disclosure policies that originate from the patient, the law, or an organization, in an interoperable manner within an HIE environment, so that individually identifiable health information may be appropriately shared for:

- Patient treatment and care coordination
- Third party payment
- Analysis and reporting for operations, utilization, access quality, and outcomes
- Public health reporting
- Population health, technology assessment and research

**Purpose and Goals:** To demonstrate with a pilot project the ability of providers to share portions of an EHR while not sharing others, such as information related to substance abuse treatment, which is given heightened protection under the law.

HIE=Health Information Exchange
HER=Electronic Health Record
DS4P Pilot

The DS4P Pilot will exercise defined aspects of health care information exchange in a real-world setting. The pilot evaluates not only the technology framework and HL7 standards, but also provides a test bed to evaluate the interaction of technology, implementation support, and operational infrastructure required to meet Data Segmentation Use case objectives at the stakeholder or organization levels.

Value Statement:
The DS4P Initiative intends to enable the privacy-protected sharing of patient data in compliance with policy, regulation, and patient consent directives. The goal is to build patient trust and participation in the health care system.

Disclaimer: This Pilot demonstration does not represent the official position or policies of the ONC, the Substance Abuse and Mental Health Services Administration, or the Department of Veterans Affairs. This Pilot demonstration is for educational purposes only and does not constitute legal advice or opinion.
Sending and Receiving “Pushed” Messages

**Sending Organization**

1. Verify that the Receiving Organization is authorized for the level of protected health information to be sent and determine restrictions that exist on use following delivery.

2. Provide document classification information as ACI (Access Control Decision Information) and appropriately mark document sections with overall classifications.


**Receiving Organization**

4. Document set received and processed by Receiving Organization.

5. Verify that the Receiving Organization user is authorized access to the information inherent in organizational policy restrictions and the information classification markings.
Demonstration Ecosystem

Phase I – Push Scenarios

Consent Directive Management

Patient Authorization And Restrictions

HIPAA

Mitre

Patient Consent Directive Attributes

Enforce Release Constraints

AuthZ Decision Request

Enforce Internally

XACML PDP
Enforcement
Patient Sensitivity Constraints/Obligations
Organizational/Jurisdictional/Applicable Privacy Law
Obligations and Refrain Policies

Jericho Systems

SAMHSA

VA

Patient Information (C-32)

Consent Locator
Access Control System (ACS)
Clinical Rules
Organizational Rules
Annotation Policy
Collection Policy
Redisclosure Policy
Push Receiver
XDS and XD*
PUSH Receiver
Audit Services
Demonstration Harness

Sending Organization

Receiving Organization

REM Reference ‘EHR’
PUSH SENDER
HCS/ACS
ORCHESTRATION
HCS Rules Engine
HCS Document Processing (Tagging)
XDM Metadata and Packaging

AuthZ = Authorization
ACS = Access Control System
HCS = Health Care Classification System
PDP = Policy Decision Point

Enforce Constraints on Re-Disclosure

Prototypic Third Party

9/7/2012
Wrapping for Transmission and Processing upon Receipt

Sending Organization

- Document Set Prepared for Delivery to Receiving Organization

Layered Security Service

- Document Assembly and Tagging
- Create Secured Inner Policy Wrapper
- Create Secured Outer Policy Wrapper
- Create Composite Document Set

Receiving Organization

- Document Set Delivered to and Processed by Receiving Organization

Layered Security Service

- Open to Expose Composite Document Set
- Open Secured Outer Policy Wrapper
- Open Secured Inner Policy Wrapper

Document Set/ACI Extraction

- Process Classification System Attributes from Wrappers and Received Document

Apply Classification System Attributes to Document and Wrappers

9/7/2012
Decryption Process

Decryption of Composite Document Set

- No Obligations
  - No Obligations
  - One to Many Obligations

Traditional Key Exchange

Access Control System Interactions

Key Management Key Exchange

Originating Service Organization
Access Control Policy Components

Adapted from Organization for Advancement of Structured Information Standards (OASIS) eXtensible Access Control Markup Language (XACML) version 2.0
Access Control Policy Example

Policy

- Fetch Rule: If external user, then audit each access occurrence
- Rule Combining Algorithm: Only Rules with POU = Subject(POU) = Treatment and PatientID = John Doe 12345

Rule

- Effect: Permit
- Condition: Is Subject(Role) a licensed healthcare provider? Is Subject(LOA) > 3? Is Subject(Functional Group) = Resource(PatientID = Joe Doe 12345) Care Team? Is Subject(Location) within Environment location?
- If Resource(PatientID = John Doe 12345) includes Summary of Care with Alcohol Abuse Condition Entry, then Subject(Role) = PCP? If Resource includes Alcohol Abuse Condition Entry, then Subject(sensitivity) = ETH?

Target

- Action: Read, EHR(PatientID = yyy)
- Resource: EHR(PatientID = John Doe 12345)
  - Problem List*
  - Immunizations
  - Allergies
  - Medications*
  - History*
  - Classification Markings**
    * Includes ETH Condition
    ** Confidentiality = R, Sensitivity = ETH (42 CFR Part 2), POU = Treatment

- Subject: Legal Name, email, X509 Name, Subject(POU) = Treatment, Subject(Role) = PCP, Subject(LOA) = 4, Subject(Functional Group) = Care Team(PatientID = John Doe 12345)
- Environment: Location = USA
### Key Resource Access Control Decision Information

<table>
<thead>
<tr>
<th>Resource or Resource Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>The identity of the entity to which access is attempted</td>
</tr>
<tr>
<td>EHR, Named Patient Record, Workflow (e.g. Orders)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Individual Initiator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control Identity and Accesses allowed or denied on target</td>
</tr>
<tr>
<td>Connect, Access Control Lists</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hierarchical Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hierarchical Group identities and the accesses allowed or denied to them</td>
</tr>
<tr>
<td>Organizational Headquarters/enterprise wide access</td>
</tr>
<tr>
<td>Geographical Sub-division/Sub-division access, Accesses restricted to Local Hospital, etc.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Functional Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Healthcare Work Group identities and accesses allowed or denied</td>
</tr>
<tr>
<td>Care Team can see assigned patients, Pharmacy can see &quot;Pharmacy Only&quot; data, Clinic, etc.</td>
</tr>
</tbody>
</table>

### Role(s)

- Role identities and the accesses on the target allowed or denied to them
- Structural (Coarse-grain) Roles: Oncologist, Dentist, etc. without further qualifiers and/or
- Functional (Fine-grain) Roles defined by a named Permission Set, e.g.,
- Role Name::{{Perm1, Perm2...PermN}}
- Where permissions are "actions" allowed on specific "information objects", for example:
  - WRITE Progress Note
  - WRITE Medication Order
  - SIGN Prescription

### Security Labels

- Data tags to which access is allowed
- Security Clearance, Confidentiality Code (e.g. Very Restricted), Sensitivity Code (e.g. HIV, Sickle Cell)

### Integrity Markings

- Target integrity levels and accessses allowed or denied to them
- Read Unsigned Progress Notes, etc.

### Authorities

- Individual authority identities and the accesses allowed or denied to them
- HQ Staff, Auditor, Law Enforcement

<table>
<thead>
<tr>
<th>Policy Environment:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entity, Role, Rule, Attribute Based Access Control</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Access Control Mechanisms:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capability, ACL, Label, or Context Based</td>
</tr>
</tbody>
</table>

Adapted from: ISO/IEC 10181-3
Security Labels Based on HL7 Standard Vocabulary
HL7 Healthcare Privacy & Security Classification System (HCS) Sept 2012 Ballot

- Standard, semantically interoperable metadata used to classify healthcare information
- Enables appropriate access control decisions at each layer of security services

Enforces Privacy Policies Governing:
- End users within the custodian’s enterprise
- Custodian disclosure of segmented data by redaction, masking, and encryption of content “payload”
- Access to business (inner) and transport (outer) envelopes to minimize payload disclosure
- Intermediaries’ receipt, storage, routing, and redisclosure
- Access, use, and any further redisclosure by end users within the receiver’s system
Healthcare Classification System for Security and Privacy

Common Vocabulary for Policy Design, Management, Communication, and Runtime Enforcement
Data Sensitivity Tagging & Masking

Example

Annotation Rule That Executes

```xml
<entryRelationship>
  <observation>
    <templateId root="2.16.840.1.113883.10.20.1.50"/>
    <code code="33999-4" codeSystem="2.16.840.1.113883.6.1" display="Status"/>
    <statusCode code="completed"/>
    <value code="55561003" codeSystem="2.16.840.1.113883.6.96" display="Active" xsi:type="CE">
      <originalText>
        <reference value="#PROBSTATUS_0"/>
      </originalText>
      <value/>
    </value>
    </observation>
  </entryRelationship>
</entryRelationship>
```

Use of CDA R2 Entry Level External Reference
DS4P Pilot Success Metrics

- The Pilot has demonstrated and tested privacy-protected exchange of clinical records including:
  - Automate Data Tagging (Purpose of Use, Data Confidentiality, Data Sensitivity) per Classification Scheme (HL7 Information Model Terminology Standards)
  - Align with Data Segmentation Push Use Case
  - Demonstrate HIT Standards Committee Metadata Standards by:
    - Using HL7 security and privacy metadata in a CDA header for C32 envelope
    - Completing Use Case Test Cases Demonstrating Compliance with DS4P Implementation Guide
Use Case: Directed Exchange

Directed Exchange ("Push" transactions) refers to data sharing that is initiated by the sender and is NOT in response to a query.

- "Directed Exchange" does not refer to the exchange protocols defined by the Direct Project.

User Story 1(Push (Directed Exchange)/ Share All)

- Patient X enters into an inpatient Alcohol and Drug Abuse Treatment Program (ADATP).
- The Patient is notified by the ADATP that the ADATP is under legal obligation not to disclose additionally protected data without the Patient’s consent.
- The Patient indicates that he or she would like to disclose all treatment data with his or her PCP.
Use Case: Directed Exchange (cont.)

User Story 1 (Push (Directed Exchange)/ Share All)

• The Patient completes a 42 CFR Part 2-compliant consent form authorizing the ADATP to disclose the protected data with the PCP
• The ADATP staff electronically captures the Patient’s additionally protected data and Consent Directive
• The ADATP electronic system appropriately annotates the Patient’s data.
• Upon discharge, or at any time permitted by patient consent, the ADATP electronically sends (pushes) data, e.g., a CDA summary of care, which the Patient has authorized to be disclosed to the PCP, with an accompanying 42 CFR Part 2 compliant prohibition on no re-disclosure notification
• The PCP’s EHR receives and incorporates the Patient’s annotated additionally protected data, and persists the prohibition on re-disclosure notification
Each disclosure under §§ 1.460 through 1.499 of this part made with the patient's written consent must be accompanied by a written statement similar to the following:

- This information has been disclosed to you from records protected by Federal confidentiality rules (38 CFR Part 1).
- The Federal rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 38 CFR Part 1.
- A general authorization for the release of medical or other information is NOT sufficient for this purpose.
- The Federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patient or patient with sickle cell anemia or HIV infection.

9/7/2012
Legal Framework: SAMHSA 42 CFR Part 2 Prohibition on Redisclosure

Records of the identity, diagnosis, prognosis, or treatment of any patient which are maintained in connection with the performance of any program or activity relating to alcoholism or alcohol abuse education, training, treatment, rehabilitation, or research, which is conducted, regulated, or directly or indirectly assisted by any department or agency of the United States shall, except as provided in subsection (e) of this section, be confidential and be disclosed only for the purposes and under the circumstances expressly authorized under subsection (b) of this section.

- **Notice to accompany disclosure.** Each disclosure made with the patient's written consent must be accompanied by the following written statement:

  "This information has been disclosed to you from records protected by Federal confidentiality rules (42 CFR part 2). The Federal rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 CFR part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose. The Federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patient."

- Any disclosure made under these regulations must be limited to that information which is necessary to carry out the purpose of the disclosure.

- **Responding to requests.** (1) The presence of an identified patient in a facility or component of a facility which is publicly identified as a place where only alcohol or drug abuse diagnosis, treatment, or referral is provided may be acknowledged only if the patient's written consent is obtained.

- Any answer to a request for a disclosure of patient records which is not permissible under these regulations must be made in a way that will not affirmatively reveal that an identified individual has been, or is being diagnosed or treated for alcohol or drug abuse.

**Disclaimer:** This Pilot demonstration does not represent the official position or policies of the ONC, the Substance Abuse and Mental Health Services Administration, or the Department of Veterans Affairs. This Pilot demonstration is for educational purposes only and does not constitute legal advice or opinion.
Demonstration Participants

Access Control Service
- Policy Decision/Enforcement
- Patient Sensitivity Constraints/Obligations
- Organizational/Jurisdictional/Applicable Privacy Law
- Obligations and Refrain Policies

Jericho Systems

Consent Directive Attributes

HIPAAT

MITRE

SAMHSAN

Sending Organization

AuthZ Decision Request

VA

Receiving Organization

Consent Directive Management

Enforce Constraints

Patient Information (C-32)