Presentation to HL7
*S&I Framework Data Segmentation for Privacy Initiative*

9/25/2013

Johnathan Coleman, CISSP

Initiative Coordinator, Data Segmentation for Privacy

OCPO/ONC/HHS (CTR)

Tel: (843) 647-1556  jc@securityrs.com
Presentation Agenda

• Purpose and Need for DS4P
• Technical Approach/Building Blocks
• S&I DS4P Initiative Artifacts
• Selected Standards
• Questions
Data Segmentation for Privacy

PURPOSE/NEED FOR DS4P
Why Segment Data?

The Need for Data Segmentation

• Some healthcare information requires special handling that goes beyond the protection already provided through the HIPAA Privacy rule, which allows health care providers to disclose protected health information without patient consent for treatment, payment and health care operations purposes.

• Protection through the use of data segmentation emerged in part through state and federal privacy laws which address social hostility and stigma associated with certain medical conditions.*

* The confidentiality of alcohol and drug abuse Patient records regulation and the HIPAA privacy rule: Implications for alcohol and substance abuse programs; June 2004, Substance Abuse and Mental Health Services Administration.
According to recent estimates posted on healthit.gov:

• An estimated 26% of Americans age 18 and older are living with a mental health disorder in any given year.
• 46% will have a mental health disorder over the course of their lifetime.
• An estimated 8% of Americans are in need of drug or alcohol abuse treatment.
• Patients suffering from serious mental illness have increased rates of co-occurring conditions, which results in a reduced life expectancy of 8-17 years.
Heightened Legal Privacy Protections in scope for the S&I DS4P Initiative:

- **42 CFR Part 2**: Federal Confidentiality of Alcohol and Drug Abuse Patient Records regulations protect specific health information from exchange without patient consent.
- **Title 38, Section 7332, USC**: Laws protecting certain types of health data coming from covered Department of Veterans Affairs facilities and programs. Types of data include sickle cell anemia, HIV, and substance abuse information.
Other Examples of Heightened Legal Privacy Protections

- **45 CFR §164.522(a)(1)(iv):** Effective 3/26/2013, this final rule describes how patients may withhold any health information from health plans for services they received and paid for out-of-pocket.*

- **Other State and Federal laws** relating to certain conditions or types of data, including:
  - Mental Health
  - Data Regarding Minors
  - Intimate Partner Violence and Sexual Violence
  - Genetic Information
  - HIV Related Information.

* May be useful, but patient, not provider, has responsibility for ensuring that downstream recipients know that patient is requesting restriction.
The Patient receives care at their local hospital for a variety of conditions, including substance abuse as part of an Alcohol/Drug Abuse Treatment Program (ADATP).

Data requiring additional protection and consent directive are captured and recorded. The patient is advised that the protected information will not be shared without their consent.
A clinical workflow event triggers additional data to be sent to Provider/Organization 2. This disclosure has been authorized by the patient, so the data requiring heightened protection is sent along with a prohibition on redisclosure.

Provider/ Organization 2 electronically receives and incorporates patient additionally protected data, data annotations, and prohibition on redisclosure.
Data Segmentation for Privacy

TECHNICAL APPROACH
Layered Approach for Privacy Metadata

• “Russian doll” concept of applying metadata with decreasing specificity as layers are added to the clinical data.

• Privacy metadata uses standards to convey:
  – Confidentiality of data in clinical payload
  – Obligations of receiving system
  – Allowed purpose of use
Types of Privacy Metadata used by DS4P

- **Confidentiality Codes:**
  - Used by systems to help convey or enforce rules regarding access to data requiring enhanced protection. Uses “highest watermark” approach.

- **Purpose of Use:**
  - Defines the allowed purposes for the disclosure (e.g. Treatment, Emergency Treatment etc).

- **Obligations:**
  - Refrain Codes: Specific obligations being placed on the receiving system (e.g. do not re-disclose without consent)
Technical Approach

Requirements of Sending System

- LOINC Document Type/Datatype for CDA
- ASC X12 4010/5010 for Healthcare Provider & facility types and Healthcare Coverage Type
- SNOMED-CT for Protected diagnoses/problems

- Identify Information that is further restricted
- ASC X12 4010/5010 for Healthcare Provider & facility types and Healthcare Coverage Type
- SNOMED-CT for Protected diagnoses/problems

- Verify the patient’s privacy consent allows the disclosure of protected information
- Query for consent directive location (optional)
- Query for consent directive (optional)
- HL7 IG for CDA, Release 2: Consent Directives, Release 1

- Add privacy metadata to health information to be disclosed to other organization
- HL7 Confidentiality Code: for CDA (N,R,V)
- HL7 Refrain Code: (e.g. prohibition on re-disclosure without consent)
- HL7 Purpose of Use: The purpose for the information disclosure (e.g. support treatment, payment, operations, research, etc.)
- URL or XACML Pointer for Policy Reference if needed

SENDING SYSTEM: Provider/Healthcare Organization A
Data Segmentation for Privacy Initiative

DS4P ARTIFACTS
Initiative Artifacts

- Data Segmentation for Privacy Use Case document.
- Implementation Guide describing recommended standards for privacy metadata, organized by transport mechanism:
  - SOAP: Provides support for NwHIN / eHealth Exchange.
  - SMTP: Provides support for DIRECT (e.g. S/MIME, or XDR and XDM Messaging for bridging Direct and Exchange environments).
  - REST: HL7 hData Record Format or IHE Mobile Access to Health Documents (MHD) Profile.
- Analysis of HITSC recommendations for privacy metadata supporting the PCAST vision for tagged data elements.
- Executive Summary Document (Community Draft)
- DS4P IG Test Procedures
Strong Community Participation:

- Over 300 Participating Individuals
- 98 Committed Members
- 92 participating Organizations

- 6 Pilots (1 Federal, 5 Industry):
  - VA/SAMHSA (Demonstrated at HIMSS 2013 Interoperability Showcase)
  - NETSMART (Demonstrated at HIMSS 2013 Interoperability Showcase)
  - Software and Technology Vendors' Association (SATVA)
  - Jericho / University of Texas
  - Greater New Orleans Health Information Exchange (GNOHIE)
  - TeraDact
• **HL7 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1**
• Ballot Dates: August 12 – September 16, 2013
• ONC DS4P Implementation Guide (IG) are being used as core input into the HL7 DS4P IG project.
• The HL7 IG identifies the normative standards that it constrains, and a description of how the IG is compliant with its base normative standards.
• The HL7 IG includes adequate implementation guidance to developers. All IG non-HL7 standards (including vocabulary) are identified and any gaps addressed, e.g., as future harmonization proposals or as requests to appropriate SDOs
Data Segmentation for Privacy Initiative

SELECTED STANDARDS
<table>
<thead>
<tr>
<th>Capability</th>
<th>Standard/Profile</th>
<th>Specific Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td><em><em>IHE XD</em> Profiles</em>*</td>
<td>IHE XDR and XDM Metadata</td>
<td>IHE XDS Metadata used as the mechanism to support both SubmissionSet and Document metadata</td>
</tr>
<tr>
<td><strong>Vocabularies</strong></td>
<td>ASC X12 5010</td>
<td>Used to define type of insurance coverage</td>
</tr>
<tr>
<td></td>
<td>Healthcare Facility Type Value Set – as defined in HITSP C80</td>
<td>Used to define facility types (and used by systems to determine protected facilities)</td>
</tr>
<tr>
<td></td>
<td>HL7 RefrainPolicy</td>
<td>Used to convey specific prohibitions on the use of sensitive health information</td>
</tr>
<tr>
<td></td>
<td>HL7 PurposeofUse</td>
<td>Used to convey a purpose of use</td>
</tr>
<tr>
<td></td>
<td>HL7 BasicConfidentialityCodeKind</td>
<td>Used to represent confidentiality codes</td>
</tr>
<tr>
<td></td>
<td>HL7 ObligationCode</td>
<td>Used to convey specific obligations</td>
</tr>
<tr>
<td></td>
<td>HL7 ActPolicyType</td>
<td>Used to convey a type of policy</td>
</tr>
<tr>
<td></td>
<td>HL7 SensitivityPrivacyPolicy</td>
<td>Used to convey the sensitivity level of a specific policy</td>
</tr>
</tbody>
</table>
## Selected Standards

<table>
<thead>
<tr>
<th>Capability</th>
<th>Standard/Profile</th>
<th>Specific Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport</td>
<td>SOAP</td>
<td>Transport-level security</td>
</tr>
<tr>
<td>Transport</td>
<td>SMTP and S/MIME</td>
<td>S/MIME attributes are bound to SMTP to provide for the use of secure email as</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the transport mechanism for exchanging patient data</td>
</tr>
<tr>
<td>Conveying Identity</td>
<td>- Cross-Enterprise User Assertion (XUA)</td>
<td>IHE XUA Metadata</td>
</tr>
<tr>
<td></td>
<td>- OASIS SAML Specification Version 2.0</td>
<td>SAML Assertion (SAML Request and Response)</td>
</tr>
<tr>
<td>Conveying Identity</td>
<td>X.509 Digital Certificates</td>
<td>PKI to support Direct implementations</td>
</tr>
<tr>
<td>Patient Consent</td>
<td>HL7 Implementation Guide for CDA®, Release 2: Consent</td>
<td>Provides representations for expressing privacy preferences and exchanging</td>
</tr>
<tr>
<td>Structure</td>
<td>Directives, Release 1</td>
<td>privacy policies that can be enforced by consuming systems</td>
</tr>
</tbody>
</table>
The full whitepaper by Melissa M. Goldstein, entitled, “Data Segmentation in Electronic Health Information Exchange: Policy Considerations and Analysis” is available at:
http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__privacy_and_security/1147

Thank you!

Johnathan Coleman, CISSP, CISM
Initiative Coordinator, Data Segmentation for Privacy
Principal, Security Risk Solutions Inc.
698 Fishermans Bend,
Mount Pleasant, SC 29464
Email: jc@securityrs.com  Tel: (843) 647-1556

Scott Weinstein, J.D.
Office of the Chief Privacy Officer
Office of the National Coordinator for Health Information Technology
Department of Health and Human Services
Email: scott.weinstein@hhs.gov