Putting the I in Health IT
www.HealthIT.gov

U.S. Department of Health & Human Services

Report to the HITSC Privacy and Security Work Group

S&I Framework Data Segmentation for Privacy Initiative

3/20/2013

Presentation Agenda

- Overview of the DS4P Approach
  - Purpose and Need for DS4P
  - Technical and Policy Challenges
  - Technical Approach/Building Blocks
  - Selected Standards
- DS4P Initiative Accomplishments/Artifacts
- Recommendations
- 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.

Why Segment Data?

Examples of Heightened Legal Privacy Protections

- **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.
- **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.*

* May be useful, but patient, not provider, has responsibility for ensuring that downstream recipients know that patient is requesting restriction.

Why Segment Data?

Examples of Heightened Legal Privacy Protections

- While the Data Segmentation for Privacy Initiative focused on types of data requiring enhanced protection under these laws, the principles are extensible to a broader range of privacy policies than those included in this presentation.
- For example, State and Federal laws exist to protect data related to select conditions/types of data, including:
  - Mental Health
  - Data Regarding Minors
  - Intimate Partner Violence and Sexual Violence
  - Genetic Information
  - HIV Related Information.

Data Segmentation for Privacy

TECHNICAL CHALLENGES

Technical Challenges

- **How to Segment:** There are multiple levels at which segmentation can occur (e.g. disclosing provider, intended recipient, or category of data such as medications). There have been no widely adopted standards to segment at these levels or for transferring restrictions across organizational boundaries (e.g. for re-disclosures).
- **Unstructured Data:** Prevalence of free-text complicates identification of data subject to enhanced protection.
- **Granularity:** Lack of granularity in current implementations (e.g. opt-in/out) results in reliance on out-of–band handling (all-or-nothing choice is technically easier for organizations to manage).

Data Segmentation for Privacy

TECHNICAL APPROACH

Technical Approach

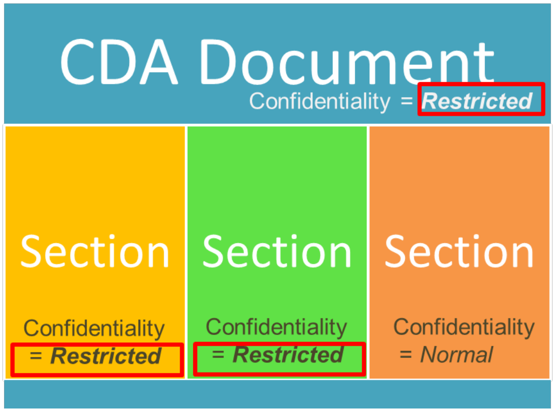
Layered Approach for Privacy Metadata

- "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

Technical Approach

Types of Privacy Metadata used by DS4P



CDA Document
Confidentiality = *Restricted*

Section
Confidentiality = *Restricted*

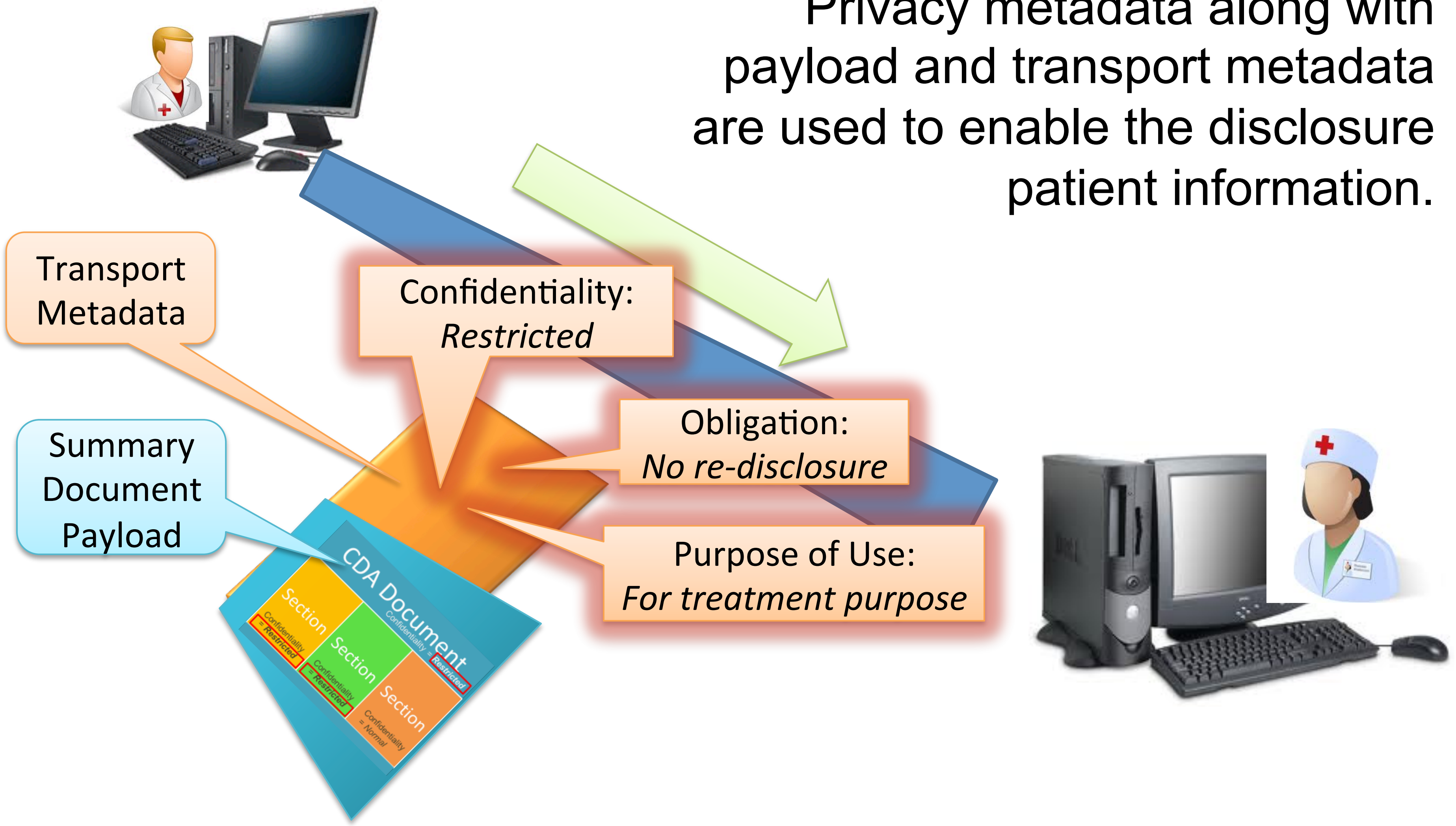
Section
Confidentiality = *Restricted*

Section
Confidentiality = *Normal*

- 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

Privacy metadata along with payload and transport metadata are used to enable the disclosure patient information.



Transport Metadata

Confidentiality: *Restricted*

Obligation: *No re-disclosure*

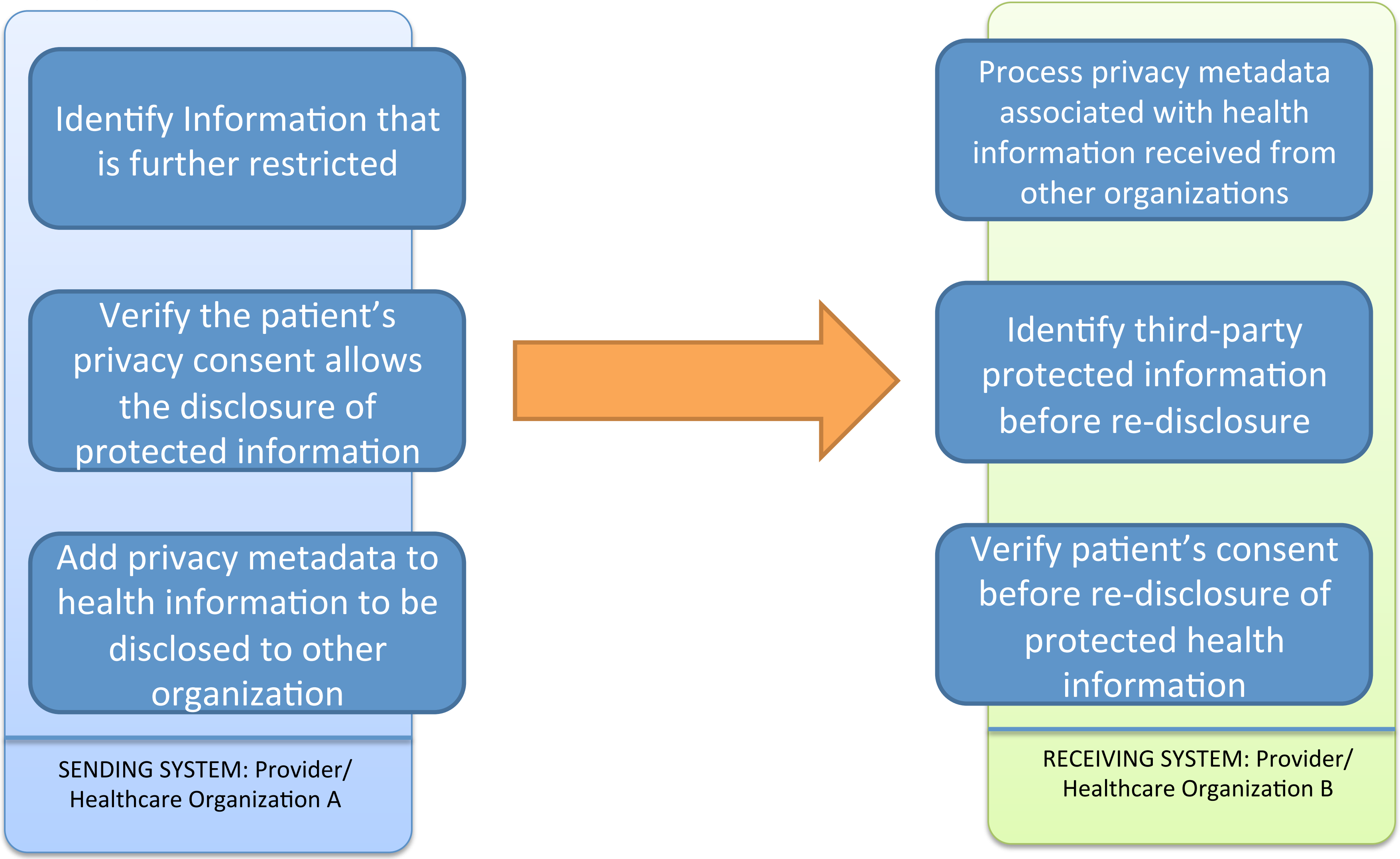
Purpose of Use: *For treatment purpose*

Summary Document Payload

CDA Document
Confidentiality = Restricted
Section
Confidentiality = Restricted
Section
Confidentiality = Restricted
Section
Confidentiality = Normal

Technical Approach

System Behavior



Identify Information that is further restricted

Verify the patient's privacy consent allows the disclosure of protected information

Add privacy metadata to health information to be disclosed to other organization

SENDING SYSTEM: Provider/ Healthcare Organization A

Process privacy metadata associated with health information received from other organizations

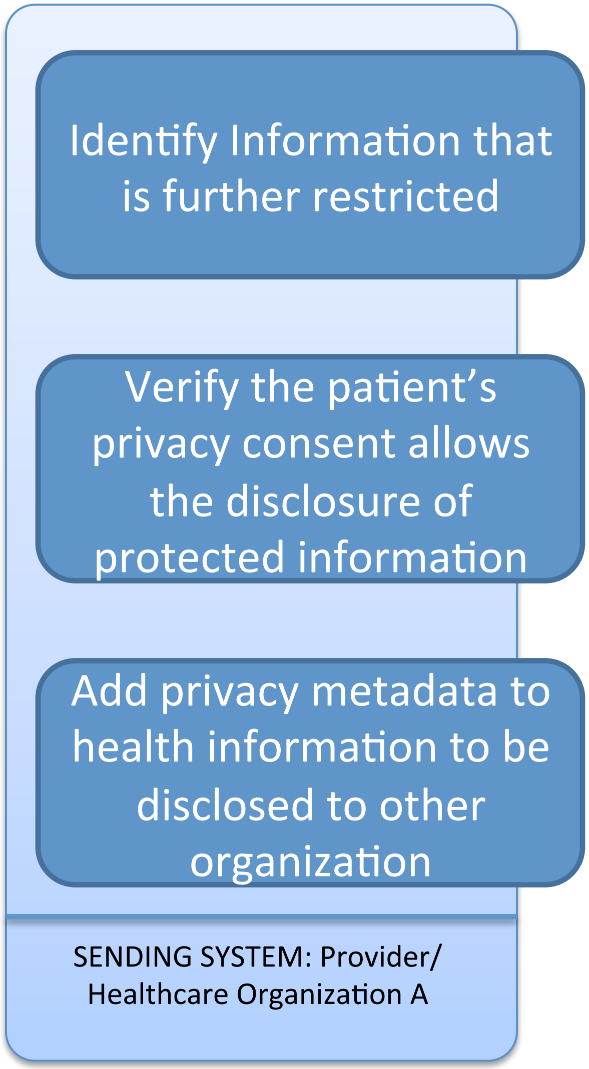
Identify third-party protected information before re-disclosure

Verify patient's consent before re-disclosure of protected health information

RECEIVING SYSTEM: Provider/ Healthcare Organization B

Technical Approach

Requirements of Sending System



Identify Information that is further restricted

- 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

Verify the patient's privacy consent allows the disclosure of protected information

- Query for consent directive location (optional)
- Query for consent directive (optional)
- Check HL7 CDA R2 PCD

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

SELECTED STANDARDS

Technical Approach

Confidentiality Codes:

- The DS4P initiative uses HL7 confidentiality code vocabulary as part of its implementation guide using the constrained value set specified by the C-CDA.
- CDA restricts Confidentiality Code to value set *BasicConfidentialityKind*
- Only Very Restricted (V), Restricted (R) or Normal (N) codes may be used

Technical Approach

Purpose of Use:

- HL7 PurposeOfUse conveys the rationale or purpose for an act (e.g. TREAT or ETREAT).
- Used in the context of a request for information (e.g. SAML Assertion)
- *May also be used in a push/DIRECT environment in the form of HL7 POU codes in the XD* metadata*
- The need for ensuring consistency between the request (if applicable) and the disclosure of data in accordance with the consent.

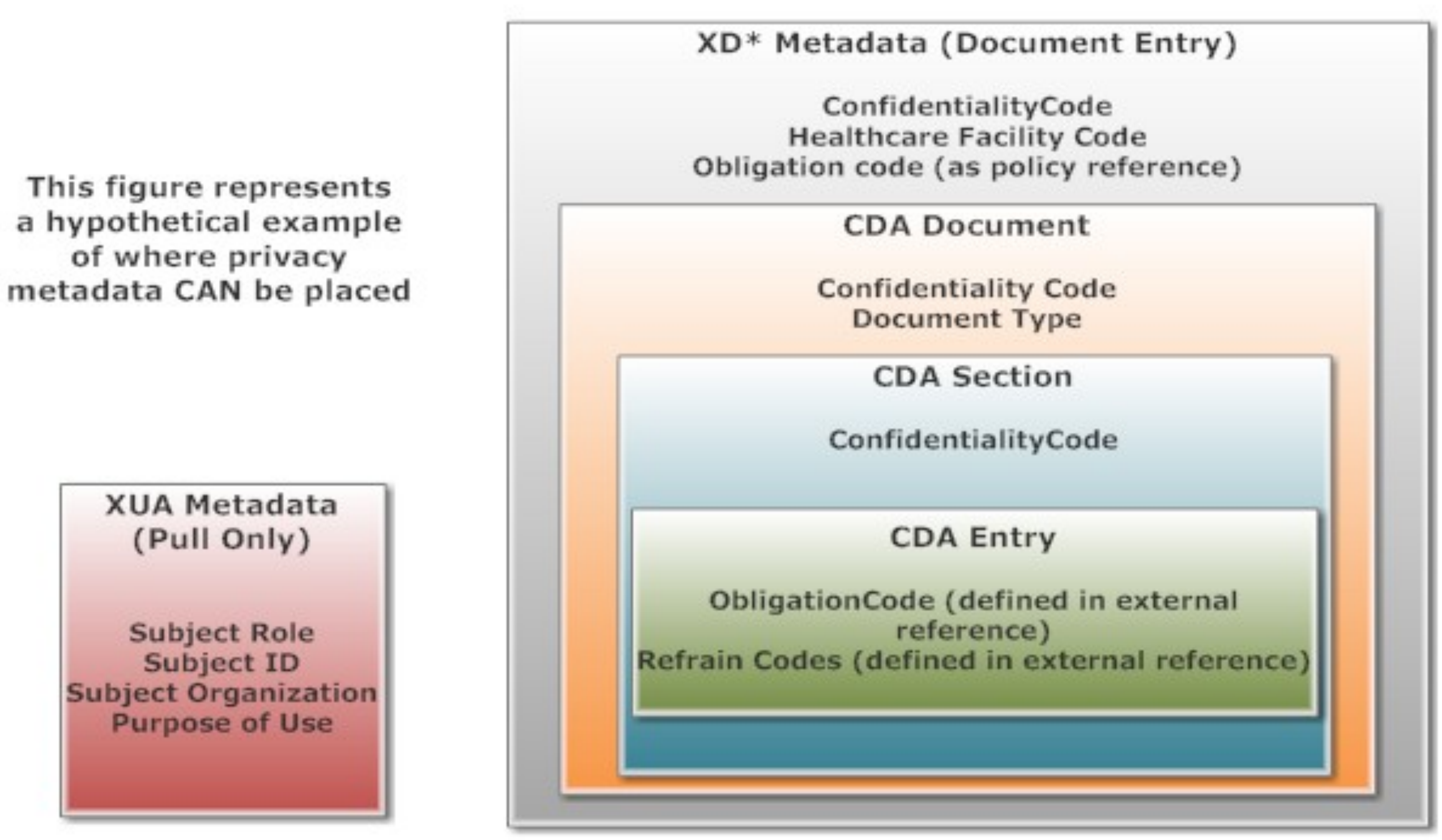
Technical Approach

Obligations:

- **Refrain Policy:** HL7 RefrainPolicy conveys prohibited actions which an information custodian, receiver, or user is not permitted to perform unless otherwise authorized or permitted under specified circumstances
- Typical DS4P value is NORDSCLCD = Prohibition on redisclosure without patient consent directive)

- **Obligation Policy:** May also be used to provide additional instructions for the receiver to know how to handle information

Technical Approach



This figure represents a hypothetical example of where privacy metadata CAN be placed

XUA Metadata (Pull Only)

Subject Role
Subject ID
Subject Organization
Purpose of Use

XD* Metadata (Document Entry)

ConfidentialityCode
Healthcare Facility Code
Obligation code (as policy reference)

CDA Document

Confidentiality Code
Document Type

CDA Section

ConfidentialityCode

CDA Entry

ObligationCode (defined in external reference)
Refrain Codes (defined in external reference)

Selected Standards

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

Selected Standards

Capability	Standard/Profile	Specific Usage
Transport	SOAP	Transport-level security
Transport	SMTP and S/MIME	S/MIME attributes are bound to SMTP to provide for the use of secure email as the transport mechanism for exchanging patient data
Conveying Identity	- Cross-Enterprise User Assertion (XUA) - OASIS SAML Specification Version 2.0	IHE XUA Metadata SAML Assertion (SAML Request and Response)
Conveying Identity	X.509 Digital Certificates	PKI to support Direct implementations
Patient Consent Structure	HL7 CDA R2 Consent Directive (DSTU)	HL7 CDA Consent Directive DSTU

Data Segmentation for Privacy Initiative

ACCOMPLISHMENTS/ARTIFACTS

Initiative Accomplishments

DS4P Deliverables:

- 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

Initiative Accomplishments

Strong Community Participation:

- 297 Participating Individuals
- 98 Committed Members
- 92 participating Organizations

- 5 Pilots (1 Federal, 4 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)

Initiative Accomplishments

VA/SAMHSA Pilot

(includes MITRE, HIPAAT, and Jericho Systems)

- SAMHSA is extending/continuing development of their open source Access Control Service (ACS) by adding an "informed consent" user interface, by adding API's to manage identities of patients and providers (e.g. Kantara & NSTIC), and by pilot testing a production grade ACS with at least one Health Information Exchange (HIE). The target date to begin pilot testing is October, 2013.
- SAMHSA is also translating privacy protection policies into standardized clinical & social service terminology. This is being done through HL7 ballots of the Summary Behavioral Health Record and Implementation Guide, and the Privacy Consent Implementation Guide.
- SAMHSA is also able to implement privacy protections in the context of public health reporting or research by permitting or redacting more or less demographic/identity data. This second form of segmentation is pertinent to the new Structured Data Capture (SDC) S&I Initiative.

Initiative Accomplishments

SATVA Pilot:

Includes Cerner Anasazi, Valley Hope Association, Defran Systems, Inc. and HEALTHeLINK

- Software and Technology Vendors Association (SATVA) pilot implemented options available in the DS4P IG into a specific implementation of:
  - incorporation of the human readable narrative notices into disclosures
  - incorporation of legally and contractually required obligation and refrain codes at the envelope, header and entry level of disclosures in both human and machine readable format.
- SATVA's approach to Scenario #3, using a HIE, is to communicate the CCD to the HEALTHeLINK RHIO in the Buffalo, NY region and are within a few weeks of going into production.
- The Valley Hope Association member of the eco-system will also begin deployment of the capturing of consents online, using a browser application, and management of Part 2 compliant disclosures using the SATVA model.

Initiative Accomplishments

NETSMART Pilot:

Includes Tampa Bay (2-1-1) Referral Network and Kansas HIE (KHIN)

- Enhancements to the HIE and EHR solutions used in this pilot focused on:
  - Ensuring that all data is correctly tagged in the payload and the protocols used to transport the payload.
  - The receiving HIO or EHR can properly enforce the policies associated with the sensitive nature of the data received.
- The solution is being implemented with two different groups :
  - The referral network in the Tampa Bay (2-1-1) will implement the first two scenarios, managing the direct push or pull of information between the various organizations involved in the coordination of care of an individual.
  - The Kansas HIE (KHIN) along with behavioral health providers in their network will implement scenario 3, introducing the registry and repository model to the pull of information.
- Each of these groups will manage restricted data associated with programs regulated by 42 CFR part 2 and ensure that all requirements of this regulation are met.

Initiative Accomplishments

Jericho Systems / University of Texas Pilot:

Goals:

- The Pilot involves the exchange of simulated Electronic Health Records (EHR) between large healthcare providers using Nationwide Health Information Network (NwHIN) Information Technology (IT) standards.
- Each access request over eHealth Exchange will be decided in real time based on computable policy that includes privacy metadata.
- Patient consent directives (PCD) will be included in the evaluation of the access request.
- The Pilot will explore three aspects of this exchange:
  - How is the PCD correlated with the patient identity;
  - How is the PCD retrieved for use in the access control decision; and
  - How is the consumer informed of the request and access control decision.

Initiative Accomplishments

Greater New Orleans HIE (GNOHIE) Pilot:

Accomplishments

- Filtering of sensitive data from entering the CDR
- Exchange of filtered information among community member organizations
- Mapping of data in CDR that does not include any sensitive elements
- Establishment of sensitive data framework in accordance with Louisiana law that accounts for SAMSHA and genetic testing elements
- Alignment of sensitive data framework with N, R, V standard codes

Next steps for the pilot

- Integrating previously filtered sensitive data into the CDR
- Appropriate mapping of integrated data
- Assignment of the mapped sensitive data to specific segments of confidentiality, N, R, V as established by the community governed sensitive data policy
- Exchange of information hosted in the integrated CDR that accords with the community governed sensitive data policy

Data Segmentation for Privacy Initiative

CONCLUSION

Conclusion (1)

- Data segmentation provides a means for protecting specific elements of health information, both within an EHR and in broader electronic exchange environments, which can prove useful in implementing current legal requirements and honoring patient choice.

- While there is still work to be done and we have yet to see the full outcomes of the pilots, we are hopeful that data segmentation will facilitate improved sharing and integration of behavioral health information among providers.

Conclusion (2)

- Extensions to some base standards and adoption/refinement of the DS4P Implementation Guides by the standards community will help accelerate adoption and allow interoperable solutions for appropriate privacy protection to be implemented.
- We hope data segmentation will give patients confidence that any privacy choices they make - which are allowed by law, jurisdictional or organizational policy – will be honored.

References/Contact Information

- 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

Ioana Singureanu, MS
Standards SME, Data Segmentation for Privacy
Principal, Eversolve LLC
8 Woodvue Road, Windham, NH 03087
Email: ioana.singureanu@gmail.com
Tel: (603) 548 5640

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

Data Segmentation for Privacy Initiative

BACKUP SLIDES

Initiative Accomplishments

VA/SAMHSA Pilot:

- **Stakeholders & Points of Contact**
  - **SAMHSA -** Richard Thoreson
    REM Reference 'EHR', PUSH Sender, HCS/ACS Orchestration, HCS Rules Engine, HCS Document Processing(Tagging)
  - **VA** - Mike Davis
    Consent Locator, Access Control System(ACS), Clinical Rules, Organizational Rules, Push Receiver, XDS and XD*,Re-Disclosure ex.
  - **Mitre -** Anne Kling
    Patient Authorization and Restrictions
  - **Jericho Systems -** David Staggs
    Policy Decision Point, Enforcement, Patient Sensitivity Constraints/Obligations, Organizational/Jurisdictional Applicable Privacy Law, Obligations and Refrain Policies
  - **HIPAAT** - Kel Callahan
    Patient Consent Policy Management

Initiative Accomplishments

VA/SAMHSA Pilot:

- **Use Case Scenarios:**
  - **UC Scenario 1: User Story 1.1A**
    Section 7332 of Title 38 Push (Directed Exchange) / Share Partial
  - **UC Scenario 2: User Story 1.1B**
    Section 7332 of Title 38 Pull / Share all
  - **UC Scenario 3: User Story 1C**
    Pull
  - **UC Scenario 4: User Story 1.1C**
    Section 7332 of Title 38 Push (Directed Exchange) / Change Mind
  - **UC Scenario 6: User Story 3**
    Break the Glass

Initiative Accomplishments

SATVA Pilot:

- **Stakeholders & Points of Contact**
  - **Software and Technology Vendors Association (SATVA) and Cerner Anasazi.**
    Michael D. Morris
  - **Valley Hope Association:**
  - John Leipold MBA, DBA
  - **Defran Systems, Inc.**
    Arthur Khanlian
    HEALTHeLINK
    Margaret Cosentino

Initiative Accomplishments

SATVA Pilot:

- **Use Case Scenarios:**
  - **UC Scenario 1 : User Story 1**
    42 CFR Part 2 Push (Directed Exchange) / Share All - *Direct and XDS.b*
  - **UC Scenario 2 : User Story 1B**
    Pull / Share All - *42 CFR Part 2 Asynchronous Request / Response - Direct*
  - **UC Scenario 1 : User Story 1**
    42 CFR Part 2 Push (Directed Exchange) / Share All - *Direct and XDS.b*
  - **UC Scenario 2 : User Story 1B**
    Pull / Share All - *42 CFR Part 2 Asynchronous Request / Response - Direct*
  - **UC Scenario 3 : User Story 1C**
    42 CFR Part 2 Pull - *Internal Consent Repository*
  - **UC Scenario 6 : User Story 3**
    Break the Glass - *Using Web Portal for Recording the Part 2 Break the Glass Event*

Initiative Accomplishments

NETSMART Pilot:

- **Stakeholders & Points of Contact**
  - **Netsmart**
    Bill Connors
    Senior VP, General Manager, Behavioral Health
    Role: Project Sponsor

    Matthew Arnheiter
    VP, Innovations
    Role: Lead Technical Architect
  - **KHIN**
    Laura McCrary, Ed.D
    Role: HIE Sponsor

Initiative Accomplishments

NETSMART Pilot:

- **Use Case Scenarios:**

  Phase 1 (Production - January 2013)

  - **Scenario 1 - User Story 1**
    42 CFR Part 2 Push / Share All / Partial
    Scenario 2 - User Story 1B
    42 CFR Part 2 Pull between providers / Share All / Partial

  Phase 2 (Pilot Release - January 2013)

  - **Scenario 3 - User Story 1C**
    HIE Repository & Consent Repository

  Phase 3 (Production Release - February 2013)

  - **Scenario 3 - User Story 1C**
    HIE Repository & Consent Repository

Initiative Accomplishments

Jericho / University of Texas Pilot:

Stakeholders & Points of Contact

Jericho Systems:

[**David Staggs, JD**]

Initiative Accomplishments

Greater New Orleans HIE (GNOHIE) Pilot Participants:

Name	Role
Gaurav Nagrath	CIO, Louisiana Public Health Institute
Liam Bouchier	Associate Director, LPHI
Rahul Jain	HIT Business Analyst, LPHI
Kristin Lyman	Associate Director, Health Systems, LPHI
David Kulick	Project Coordinator, Health Systems, LPHI
Huahong Qiang	Sr. HIE Applications Developer, LPHI
Jonathan Bartels	Software Engineer, Mirth Corporation
Ed Donaldson	Interoperability Product Manager, SuccessEHS
Luis Smith	IT Analyst IV, Interim LSU Public Hospital

Initiative Accomplishments

Greater New Orleans HIE (GNOHIE) Pilot
Use Case Scenarios:

Section of IG	Specifics to Pilot
Protected Diagnosis Codes Use of Sensitivity Codes Use of Facility Types	Standardization of data elements to process for level of sensitivity based upon community or legal policy
Break the Glass	Specific policy pathway requirement, and assertion of emergency event use case as a reason for access
Section Level Tagging Document Level Tagging Metadata Tagging	Feasibility of tagging preexisting patient records in the centralized data repository in accordance with community or legal policy

Response to HITSC S&P WG

Excerpt rom 6/29/2012 Report

HITSC Recommendation	DS4P Analysis 🟩
Metadata pertaining to privacy should include: • Policy Pointer: A URL that points to the privacy policy in effect at the time the TDE is released.	• A Policy Pointer should point to a universally recognized Policy Reference to enable the consuming organizations to apply their interpretation of that policy.* • Metadata can also be used to provide some context as to why the information is protected (i.e. policy pointer/reference), as well as the special handling obligation placed on the receiver as a result of the policy.

The Policy Pointer can be included in the IHE XD metadata or in the Patient Consent Directive.

Response to HITSC S&P WG

Putting the I in Health IT
www.HealthIT.gov

Excerpt rom 6/29/2012 Report

HITSC Recommendation	DS4P Analysis
Metadata pertaining to privacy should include Content Metadata (Datatype and Sensitivity). Content Metadata that are needed to enforce current federal and state policies as well as to anticipate more granular policies that may be defined. • Datatype: Information category from a clinical perspective. • Sensitivity: Indicates special handling that may be necessary per the referenced policy.	DS4P Approach uses Datatype and Confidentiality* content metadata • Datatype as a data element refers to the document type (patient data) being exchanged. An initial list of possibly sensitive document types that would require data segmentation has been provided in the implementation guide. 🟩 • DS4P Approach leverages Confidentiality codes. Initial approaches recommended for piloting focus on using the confidentiality code specified within privacy metadata, or by using the Patient Consent Directive. 🟪

* DS4P approach uses HL7 confidentiality codes as metadata to describe sensitivity.

* Initial approaches recommended for piloting focus on using either the Patient Consent Directive as expressed using CDA or by specifying a confidentiality code within the IHE XDS/XDR/XDM metadata.

Response to HITSC S&P WG

Excerpt rom 6/29/2012 Report

HITSC Recommendation	DS4P Analysis
• Expand HL7 vocabulary for sensitivity. A proposed starter set could include: • Substance Abuse • Reproductive Health • Sexually Transmitted Disease • Mental Health • Genetic Information • Violence • Other	• The DS4P initiative will pilot HL7 confidentiality code vocabulary as part of its implementation guide using the constrained value set specified by the C-CDA (e.g. N,R,V). Rationale: (1) These codes are used as short-hand to reference the privacy policy dealing with certain conditions or problems. Enumerating these policies in a code set is not scalable as new privacy policies are introduced overtime. In the US this value set would have to be extended to include sickle cell anemia and sexually transmitted diseases and it would have to be continuously updated as new policies are added. (2) The detailed "sensitivity" codes only have value when used in the context of a privacy policy. The privacy policy is referenced in a policy pointer, which already contains all the information necessary to adjudicate the data element. Thus the "sensitive" codes are redundant.

Response to HITSC S&P WG

Excerpt rom 6/29/2012 Report

HITSC Recommendation	DS4P Analysis
• In order to provide coded values for Datatype, the LOINC codes specified in the CDA document code element are suggested. LOINC codes are suggested because they provide additional granularity.	• DS4P concurred with this recommendation and a constrained list of document types are included in the Data Segmentation for Privacy implementation guide that are specific to the requirements of data segmentation. • As recommended by the Health IT Standards Committee, document codes MUST be defined using LOINC, and Sending and receiving systems MUST be able to validate and evaluate LOINC document types to be able to implement this guide.