Integrating the Healthcare Enterprise

IHE IT Infrastructure
Technical Framework Supplement

Data Segmentation for Privacy
DS4P

Draft for Public Comment

Date: March 14, 2014

Author: IHE IT Infrastructure Technical Committee

Email: ITI@ihe.net

Please verify you have the most recent version of this document. See here for Trial Implementation and Final Text versions and here for Public Comment versions.

Foreword

This is a supplement to the IHE ITI Technical Framework 10.1. Each supplement undergoes a process of public comment and trial implementation before being incorporated into the volumes of the Technical Frameworks.

This supplement is published on March 14, 2014 for Public Comment. Comments are invited and can be submitted at http://www.ihe.net/ITI_Public_Comments. In order to be considered in development of the Trial Implementation version of the supplement, comments must be received by April 13, 2014

This supplement describes changes to the existing technical framework documents.

"Boxed" instructions like the sample below indicate to the Volume Editor how to integrate the relevant section(s) into the relevant Technical Framework volume.

Amend section X.X by the following:

Where the amendment adds text, make the added text **bold underline**. Where the amendment removes text, make the removed text ~~**bold strikethrough**~~. When entire new sections are added, introduce with editor's instructions to "add new text" or similar, which for readability are not bolded or underlined.

General information about IHE can be found at: http://ihe.net.

Information about the IHE IT Infrastructure domain can be found at: http://ihe.net/IHE_Domains.

Information about the organization of IHE Technical Frameworks and Supplements and the process used to create them can be found at: http://ihe.net/IHE_Process and http://ihe.net/Profiles.

The current version of the IHE IT Infrastructure Technical Framework can be found at: http://ihe.net/Resources/Technical_Frameworks.

CONTENTS

Introduction to this Supplement

This supplement defines a USA realm profile for support of "Data Segmentation for Privacy (DS4P)". Data Segmentation is the privacy and security concept for differentiating between data that are to be handled differently for privacy or security reasons. Data Segmentation for Privacy support in this context is the interoperability constraints to enable documents of various and different privacy and sensitivity to be communicated within a trust framework in a way that the sender can communicate necessary and specific privacy and security attributes and obligations in a way that the recipient can clearly understand them and act properly.

This profile is based on artifacts and the findings of pilot implementers of the Data Segmentation for Privacy S&I Initiative, specifically on the Use Cases developed by the stakeholder community http://wiki.siframework.org/Data+Segmentation+for+Privacy+Homepage.

The constraints in this profile are based on the implementation guidance contained in the Data Segmentation implementation guide.

The original work-item request from ONC is to provide DS4P support for RESTful. The completion of that work-item requires both this National Extension, as well as the completion of the MHD Profile. This National Extension can be used with the current MHD, or future MHD that will be adjusted to harmonize and leverage HL7 FHIR. This National Extension can also be used with XDS, XDR, XDM, and XCA and is thus re-usable and transport agnostic.

Open Issues and Questions

DS4P_001 – Will other regions accept these constraints as defined, or will they define their own country specific constraints. There is some interest from France and Canada parties, although no formal request to act. The work represented in this US Realm National Extension has been developed in expectation of other National Extensions that may follow the same pattern for conceptually data segmentation for privacy, but using realm specific vocabularies and behaviors. Public comment is encouraged from regions outside the US Realm to assure that the general concept and pattern represented is understandable and applicable with appropriate adjustments.

DS4P_002 – This supplement relies on completion of ITI-CP-690 which identifies a mechanism for encoding security-tags as identified in the HL7 Healthcare Privacy & Security Classification System (HCS). The ballot handling is currently in process, any necessary adjustments will be made post public comment and prior to trial implementation.

DS4P_005 – Can we include copies of the realm specific value-sets to ease the use of this supplement? Some vocabularies are published by HL7 FHIR and thus have a reference URL. Some vocabularies are not yet publically published and thus don't have a URL reference.

DS4P_006 – This supplement borrows text from the HL7 DS4P work. That HL7 work is still in final stages of publication. IHE needs to harmonize with the final version of the HL7 DS4P

work. This will be done post release of the HL7 work, and after IHE public comment phase. This work must be completed before Trial Implementation.

DS4P_007 – This national extension utilizes facility type code for security and privacy reasons. Therefore we should update the metadata table in TF-3:4.1.3.2-1 to also mark the facility type code as security & privacy relevant. Should this be done in this supplement, as this supplement does utilize this? Or should this update to Vol 3 be done in an independent CP as a more visible change proposal.

DS4P_008 – There is some concern about intendedRecipient being fixed at an e-mail address. This version of the supplement accepts this restriction as currently appropriate. As other specific encodings appear this restriction should be modified. The open issue is asking for community feedback on this constraint under these circumstances.

DS4P_009 – The committee requests comment on how we can add language that allows systems to declare use of this National Extension while also participating in other trust domains that do not utilize this National Extension. There is concern that as written conformance testing may be too strict and thus not allow for multiple policy domain participation with different rules.

Closed Issues

DS4P_003 – This addresses only USA Federal regulations 42 CFR Part 2, and 38 CFR Part 1. This does not address state, region, or local policy issues. See http://fairhaven.typepad.com/my_weblog/2013/12/confidentiality-code-use-cases.html

DS4P_004 – Are the value-sets open or closed? How is versioning going to be managed?

Glossary

Add the following glossary terms to the IHE Technical Frameworks General Introduction Glossary:

No new glossary terms.

Volume 4 – National Extensions

Add appropriate Country section

Editor's Note: The section numbering for Volume 4 may change prior to publication of this document for Trial Implementation due to modifications to the template.

4 National Extensions

4.I National Extensions for USA

4.I.1 Comment Submission

This national extension document was authored under the sponsorship and supervision of IHE-USA and IT Infrastructure Technical Committee, who welcome comments on this document and the IHE USA initiative. Comments should be directed to:
http://www.ihe.net/ITI_Public_Comments

4.I.2 Data Segmentation for Privacy (DS4P)

This National Extension shows how to use and interpret the Document Sharing Metadata Profiles (XDS.b, XCA, XDR, XDM, and MHD) in compliance with the requirements identified for Data Segmentation for Privacy (DS4P). Data Segmentation is the privacy and security concept for differentiating between data that are to be handled differently for privacy or security reasons. Data Segmentation for Privacy support in this context is the interoperability constraints to enable documents of various and different privacy and sensitivity to be communicated within a trust framework in a way that the sender can communicate necessary and specific privacy and security attributes and obligations in a way that the recipient can clearly understand them and act properly.

This national extension is intended to be used within a trust framework between communicating parties. This trust framework includes policy agreements to use this national extension to communicate segmented sensitive information. For each document that is communicated within this trust framework (PUSH or PULL) the following metadata constraints shall be used to communicate the highest sensitivity of the content as evaluated by the sender. The identified sensitivity level is then enforced by the recipient. Trust enforcement is expected to be defined and managed within that trust framework.

This USA National Extension addresses methods for sharing of segmented documents containing personally identifiable information (PII) as may be permitted by privacy policies or regulations. The privacy policies on which this National Extension is based do not explicitly address the clinical implications of giving patients control over the disclosure of their sensitive records. Standards development organizations are focused on the development of technical infrastructure specifications and remain agnostic on the appropriateness of a privacy policy.

Privacy policies are defined as limits on disclosure and use. Disclosure and use restrictions may originate from a patient, a service provider, or from jurisdictions where healthcare is delivered. Implementations should be prepared to extend functionality based on state, region, and local policies.

This USA National Extension is the result of a proposal from the US Department of Health and Human Services, Office of the National Coordinator for Health IT (ONC) to develop guidance

for implementation of Data Segmentation Techniques, including RESTful patterns as defined in the MHD Profile, using the standards, building blocks and principles documented in the Use Cases developed by the S&I DS4P stakeholder community, and the NwHIN SOAP/Exchange version of the S&I DS4P Implementation Guide. Furthermore, this specification draws upon and cites specific instances of U.S. law such as 42 CFR Part 2, 38 CFR Part 1, etc. These specific references are intended to profile a specific set of users operating under realm specific law and goals. Nothing in this supplement is intended to prevent adoption or customization to meet the needs of other realms.

This USA National Extension is based on artifacts and the findings of pilot implementations of the Data Segmentation for Privacy (DS4P) S&I Framework Initiative, specifically on the Use Cases developed by the stakeholder community, and the NwHIN SOAP/Exchange version of the S&I DS4P Implementation Guide. Additionally, content from the HL7 DS4P Profiles (HL7_IG_DS4P_R1_CH1_CONTENT_N2_2014JAN, HL7_IG_DS4P_R1_CH2_DIRECT_N2_2014JAN, and HL7_IG_DS4P_R1_CH3_EXCHANGE_N2_2014JAN) which in turn reference IHE XDS are noted as important companion documents. For a detailed description of the project, refer to the S&I Initiative DS4P Project Executive Summary found at http://wiki.siframework.org/Data+Segmentation+for+Privacy+Homepage.

This USA National Extension defines constraints according to the requirements captured in the Use Cases developed by the Data Segmentation for Privacy (DS4P) S&I Framework Initiative stakeholder community and additional requirements that were identified by pilot projects engaged in validating the implementation guidance developed by the DS4P S&I Framework Initiative.

Conformance to the Document Sharing Profiles (XDS.b, XDR, XDM, XCA, and MHD) is expected with the following additional constraints based on privacy policies related to the type of document and the context of the exchange (requesting user, patient, consent, document, facility, purpose, communications mechanism, etc.).

- Document Entry constraints are given in section 4.I.2.2 below. The constraints include:
  - Security tags (confidentialityCode) constraints
    - indicate the Confidentiality Level specified by using the designated HL7 Confidentiality vocabulary
    - indicate the Handling Caveats for Obligation Policy using a designated Obligation Policy vocabulary
    - indicate the Handling Caveats for Purpose of Use using a designated Purpose of Use vocabulary
    - indicate Handling Caveats for Refrain Policy using a designated Refrain Policy vocabulary

- indicate the Authoring healthcare facility type using a designated restricted healthcare facility type vocabulary
- indicate the Document practice setting type using a designated restricted practice setting vocabulary
- indicate the Low-level classification of the document (typeCode) using a designated restricted type code vocabulary

- SubmissionSet constraints are given in the section 4.I.2.3 below. The constraints include:
  - Indicated as necessary the Targeted intended recipient (intendedRecipient)
  - Indicate the Submission set creator

4.I.2.1 DS4P Document Content

Any CDA document SHOULD comply with the CDA constraints defined in the HL7 CDA Privacy Segmented Document template (templateId: 2.16.840.1.113883.3.3251.1.1)

Other content types MAY be carried.

4.I.2.2 DS4P DocumentEntry

The following constraints apply to all documents in the submissionSet.

All the designated vocabulary and value sets are defined by HL7.

4.I.2.2.1 DS4P DocumentEntry.confidentialityCode

The confidentialityCode metadata SHALL use the “HL7 Healthcare Privacy and Security Classification System (HCS)” as defined in ITI TF-3:4.2.3.2.5

4.I.2.2.1.1 DS4P Confidentiality Security Classification Label

The confidentialityCode element SHALL contain exactly one value from the codesystem 2.16.840.1.113883.5.25 (i.e., U, L, M, N, R, or V) (aka, http://hl7.org/implement/standards/fhir/v3/Confidentiality/index.html), to indicate the Confidentiality coding of the content.

The confidentialityCode may also contain other values from other codesystems for which 4.I.2.2.1.2 and 4.I.2.2.1.3 below are two examples.

The value represents the most restrictive content in the identified document (aka, High water mark).

4.I.2.2.1.2 DS4P Sensitivity Security Classification Label

The confidentialityCode SHOULD NOT contain a sensitivity indicator unless the trust framework policies indicate otherwise.

4.I.2.2.1.3 DS4P Handling Caveats Security Category

The confidentialityCode element SHALL contain any Obligation Handling Caveats deemed necessary.

If present, the Obligation values SHALL be selected from the ValueSet

HL7 ObligationPolicyCode 2.16.840.1.113883.1.11.20445

Also found at http://hl7.org/implement/standards/fhir/v3/vs/ObligationPolicy/index.html

If present, the Purpose Of Use values SHALL be selected from the ValueSet

HL7 PurposeOfUse 2.16.840.1.113883.1.11.20448

Also found at http://hl7.org/implement/standards/fhir/v3/vs/PurposeOfUse/index.html

If present, the Refrain Policy values SHALL be selected from the ValueSet

HL7 RefrainPolicy 2.16.840.1.113883.1.11.20446

Also found at http://hl7.org/implement/standards/fhir/v3/vs/RefrainPolicy/index.html

4.I.2.2.2 DS4P DocumentEntry.healthcareFacilityTypeCode

The healthcareFacilityTypeCode element contains an indicator of the type of facility that authored the document. The ValueSet designated is restricted to the subset of practice setting codes that will not disclose details about the healthcare facility that may be protected in a specific affinity domain, directed exchange, Health Information Exchange, etc. The HL7 RestrictedHealthcareFacilityTypeCode ValueSet meets this definition and is designated for this purpose.

The healthcareFacilityTypeCode element's value SHALL be selected from the ValueSet

HL7 RestrictedHealthcareFacilityTypeCode 2.16.840.1.113883.3.3251.3.2.1

This HL7 ValueSet is a dynamic ValueSet. An HL7 'dynamic' ValueSet is one that can change over time to adjust to changing policy landscapes, but is a managed ValueSet.

4.I.2.2.3 DS4P DocumentEntry.practiceSettingCode

The practiceSettingCode element contains an indicator of the type of practice setting. The ValueSet designated is restricted to the subset of practice setting codes that will not disclose details about the practice that may be protected in a specific affinity domain, directed exchange, Health Information Exchange, etc. The HL7 RestrictedPracticeSettingCode ValueSet meets this definition and is designated for this purpose. The ValueSet is derived from SNOMED-CT codes in a way consistent with prevailing privacy policies.

The practiceSettingCode element's value SHALL be selected from the ValueSet

RestrictedPracticeSettingCode 2.16.840.1.113883.3.3251.3.2.2

This HL7 ValueSet is a dynamic ValueSet. An HL7 ‘dynamic’ ValueSet is one that can change over time to adjust to changing policy landscapes, but is a managed ValueSet.

4.I.2.2.4 DS4P DocumentEntry.typeCode

The typeCode element identifies the type of document. The ValueSet designated avoids disclosing protected information. The HL7 RestrictedTypeCode ValueSet meets this definition and is designated for this purpose.

The typeCode element’s value SHALL be selected from the ValueSet

RestrictedTypeCode 2.16.840.1.113883.3.3251.3.2.3

This HL7 ValueSet is a dynamic ValueSet. An HL7 ‘dynamic’ ValueSet is one that can change over time to adjust to changing policy landscapes, but is a managed ValueSet.

4.I.2.3 DS4P SubmissionSet

The following constraints apply to the submissionSet containing the document entries

4.I.2.3.1 DS4P SubmissionSet.intendedRecipient

The intended recipient element’s value MAY contain the intended recipient. When the exchange requires an intended recipient constraint, this element SHALL be populated. This element SHALL contain the e-mail address of that intended recipient unless the trust framework identifies an alternative encoding that is acceptable.

4.I.2.3.2 DS4P SubmissionSet.author

The Submission Set Author element’s value SHALL contain at least the author of the submission set.

This element SHALL contain the e-mail address of the author of the submission set unless the trust framework identifies an alternative encoding that is acceptable.

The recipient utilizes the SubmissionSet author as the indicator of the sender for PUSH transactions, and as the provenance identifier of the submission. This information may be used by the recipient in policy decisions and enforcement.

