CP-ITI-690-06_Final Text

<same as the Log Summary field below>

IHE Change Proposal

Tracking information:

IHE Domain	IT Infrastructure
Change Proposal ID:	CP-ITI-690
Change Proposal Status:	Final Text
Date of last update:	Jan 20, 2014
Person assigned:	John F. Moehrke

Change Proposal Summary information:

Document Sharing Metadata Enhancement for Security/Privacy Tags	
Submitter's Name(s) and e-mail address(es):	ONC
Submission Date:	July 23, 2013
Integration Profile(s) affected:	Document Sharing (XDS, XDR, XDM, XDR, XCA, MHD, MPQ, DSUB, Metadata Update, ???)
Actor(s) affected:	All that use Metadata
IHE Technical Framework or Supplement modified:	IT Infrastructure Version 10
Volume(s) and Section(s) affected:	Volume 3 Section 4.2.3.2.5

CP-ITI-690-06_Final Text

<same as the Log Summary field below>

Rationale for Change:

This Change Proposal shows how to include Security/Privacy tags in Document Sharing metadata, specifically the ConfidentialityCode. The concept of Security/Privacy tags has been developed in HL7 as the "Healthcare Classification System" (HCS), which is specific to Privacy and Security classifications. Not to be confused with the many other classifications.

This Change Proposal was initially proposed by USA HHS/ONC from work done on the Data Segmentation for Privacy (DS4P) project:

> This proposal recommends the addition of three metadata elements in addition to "confidentialityCode" to support the needs of EHR systems to exchange protected data and constrains the values allowed to be assigned to "confidentialityCode" to a simple and more interoperable value set of a basic set of values.
>
> Therefore following addisional encoded elements are proposed as additions to the XDS content profile:
>
> - Purpose of use code
> - Refrain policy code
> - Obligation policy code
> - Constrain "confidentialityCode" to a basic value set rather than an entire coding system

The changes from this original proposal were to done to recognize International needs, the need to leverage existing metadata for maximum interoperability, and to harmonize with the HL7 HCS work. This HCS work defines these tags slightly differently, but they are conveying the same thing. The Refrain Policy, Obligation Policy, and Purpose of Use are all Handling Caveats.

- [1…1] Confidentiality Security Classification Label Field
- [0…*] Sensitivity Security Category Label Field
- [0…*] Compartment Security Category Label Field
- [0…*] Integrity Security Category Label Field
- [0…*] Handling Caveat Security Category Field

This CP shows how to include these all in the existing ConfidentialityCode. Through using the existing code element in this way we give meaning to the ability to encode multiple values. This model is consistent with the existing XDS.b profile, and thus will be supported by existing products. This model places all the security tags in the same place making the logic easier for an Access Control engine to find all the relevant security tags. This model is supported automatically by existing XDS and XCA queries. This model can be used universally across XDM, XDR, XDS, XCA, as well as others. This model is additionally the same model that could be implemented in DICOM (not handled here, but recognition that there is a confidentialityCode concept that accepts multiple coded values). This model is more consistent with the HCS. This model is more consistent with the work being done with MHD and FHIR.

The model of using extended slots is not impoper, XDS does allow extensions through new slots, but is these extended slots are not guaranteed to be supported by existing systems. Existing systems can choose to reject extended slots. The model using extended slots would not have been supported on Query transactions. The extended slots would have required more changes to existing systems. The extended slots place the security tags in multiple locations thus making the effort of finding the relevant security tags more difficult.

Editor: Please make the following changes to section 3:4.2.3.2.5

4.2.3.2.5 DocumentEntry.confidentialityCode

Description:

The code specifying the **security and privacy tags** ~~**level of confidentiality**~~ of the document. These codes are set by policy **of the participants in the exchange, e.g. XDS affinity domain** ~~**of the creating entity and issues related to highly sensitive documents are beyond the scope of metadata definition. These issues are expected to be addressed separately**~~. confidentialityCode is part of a codification scheme.

The confidentialityCode can carry multiple vocabulary items. HL7 has developed an understanding of security and privacy tags that might be desirable in a Document Sharing environment, called HL7 Healthcare Privacy and Security Classification System (HCS). The following specification is recommended but not mandated by IHE, as the vocabulary bindings are an administrative domain responsibility. The use of this method is up to the policy domain such as the XDS Affinity Domain or other Trust Domain where all parties including sender and recipients are trusted to appropriately tag and enforce.

- **[1…1] Confidentiality Security Classification Label Field**
- **[0…*] Sensitivity Security Category Label Field**
- **[0…*] Compartment Security Category Label Field**
- **[0…*] Integrity Security Category Label Field**
- **[0…*] Handling Caveat Security Category Field**

In the HL7 Healthcare Privacy and Security Classification System (HCS) there are code systems specific to Confidentiality, Sensitivity, Integrity, and Handling Caveats. Some values would come from a local vocabulary as they are related to workflow roles and special projects.

The decision to include a code is the responsibility of the publisher/sender (e.g., Access Control decision) and is dependent on the Policy rules and Trust Framework in place for the exchange. Use of Sensitivity tags expose the nature of the sensitivity and should be used only when the end-to-end confidentiality of the tags can be assured.

When using the HL7 Healthcare Privacy and Security Classification System (HCS):

- **The confidentialityCode SHALL contain exactly one value from the HL7 code system V:Confidentiality (@codeSystem="2.16.840.1.113883.5.25" i.e., U, L, M, N, R, or V), to indicate the Confidentiality coding of the content.**
    - **The value represents the most restrictive content in the identified document (aka. High water mark).**
- **The confidentialityCode MAY contain values from the HL7 code system V:InformationSensitivityPolicy (@codeSystem="2.16.840.1.113883.1.11.20428"), to indicate the Sensitivity coding of the content.**
    - **Multiple values are all applicable to the content. This means that a consuming system/user must have rights to all Sensitivity classes indicated.**

<same as the Log Summary field below>

- **The confidentialityCode MAY contain values from the HL7 code system V:Compartment (@codeSystem=”2.16.840.1.113883.1.11.20478”), to indicate the Compartment of the content.**
    - **Multiple values are all applicable to the content. This means that a consuming system/user must have rights to all Compartments indicated.**
- **The confidentialityCode MAY contain values from the HL7 code system V:SecurityIntegrityObservationValue (@codeSystem=”2.16.840.1.113883.1.11.20469”), to indicate the Integrity of the content.**
    - **Multiple values are all applicable to the content.**
- **The confidentialityCode MAY contain values from the HL7 code system V:SecurityControlObservationValue (@codeSystem=”2.16.840.1.113883.1.11.20471”), to address the Handling Caveats that must be applied to the use of the content.**
    - **Multiple values all applicable to the content. A consuming system must enforce all Handling Caveats indicated.**
- **Other value-sets and codesystems MAY be used as agreed between the communicating partners.**

Coding:

Each confidentialityCode is coded within an ebRIM Classification object. See section 4.2.3.1.2 for a description of coding an ebRIM Classification. There shall be zero or more ebRIM Classification containing a confidentiality code **(some profiles require at least one). ~~and~~ ~~m~~M**ultiple values of confidentialityCode are coded by specifying multiple classification objects. For the confidentialityCode metadata attribute, the classificationScheme shall be urn:uuid:f4f85eac-e6cb-4883-b524-f2705394840f.

The following example **shows two confidentialityCodes values. It specifies normal confidentiality with code “N”, display name “Normal Clinical Data”, and coding scheme “2.16.840.1.113883.5.25”, and an obligation not to reuse with code ”NOREUSE”, display name “prohibit use beyond purpose of use”, and coding scheme “2.16.840.1.113883.1.11.20471", for the DocumentEntry labeled “ExampleDocument”. ~~specifies confidentialityCode="Example confidentialityCode Value" with display name "ExampleconfidentialityCodeDisplayName" and coding scheme "Example Scheme" for the DocumentEntry labeled "ExampleDocument".~~**

```
  <rim:Classification
      classificationScheme=
      "urn:uuid:f4f85eac-e6cb-4883-b524-f2705394840f"
      classifiedObject="ExampleDocument"
      id="IdExample_046"
      objectType="urn:oasis:names:tc:ebxml-
          regrep:ObjectType:RegistryObject:Classification"
      nodeRepresentation="~~Example confidentialityCodeValue~~N"
<rim:Name>
      <rim:LocalizedString
        value="~~ExampleconfidentialityCodeDisplayName~~Normal Clinical Data"/>
</rim:Name>
  <rim:Slot name="codingScheme">
```

<same as the Log Summary field below>

```
    <rim:ValueList>
      <rim:Value>~~Example Scheme~~2.16.840.1.113883.5.25</rim:Value>
    </rim:ValueList>
  </rim:Slot>
</rim:Classification>
<rim:Classification
    classificationScheme=
    "urn:uuid:f4f85eac-e6cb-4883-b524-f2705394840f"
      classifiedObject="ExampleDocument"
    id="IdExample_046"
    objectType="urn:oasis:names:tc:ebxml-
    regrep:ObjectType:RegistryObject:Classification"
    nodeRepresentation="NOREUSE">
  <rim:Name>
    <rim:LocalizedString value="prohibit reuse beyond purpose of use"/>
  </rim:Name>
  <rim:Slot name="codingScheme">
    <rim:ValueList>
      <rim:Value>2.16.840.1.113883.1.11.20471</rim:Value>
    </rim:ValueList>
  </rim:Slot>
</rim:Classification>
```