

CROSS-DOMAIN PRIVACY ANNOTATION

REVISION 100913-1453

Conveying data element privacy attributes during
information exchange

Brian D. Handspicker, PracticalMarkets, bd@handspicker.net
Consulting New York State ITS Human Services Enterprise Architect

WHAT: Information Privacy Across Multiple Domains, Agencies, Exchange Protocols

- Child and Family Services is an Extreme Use Case
 - ▣ Education records
 - ▣ Health records
 - ▣ Family Court records
 - ▣ Foster Care records
 - ▣ Adoption records
 - ▣ Juvenile Justice & Criminal Court records
 - ▣ Protective Services records
 - ▣ Disability & Rehabilitation records

WHY: Privacy Regulations

□ HIPAA/HITECH, 42CFR part 2

- Medical Records
- Rehabilitation Records

□ FERPA

- Educational Records

□ FOIA/Privacy Act

- Identification Records

□ RFPA

- Financial Records

□ FCRA

- Credit Reports

□ COPPA

- Children's Records

□ VAWA

- Violence
- Stalking
- Cyber-stalking

□ Address Privacy

- Domestic Violence
- Victim Protection
- Witness Protection
- VIP Protection

□ Library Privacy

□ Personal Privacy

- Identity Theft
- Discrimination
- Bullying

PROBLEM: Exchange Protocols Lacked Information Privacy Support

□ HIPAA

- ▣ HL7 Data Segmentation for Privacy (DS4P)
- ▣ ONC S&I DS4P

□ FERPA

- ▣ PESC
- ▣ Ed-Fi
- ▣ SIF

□ GRA

- ▣ ebXML
- ▣ RSWS

HOW: Multiple Orthogonal Security & Privacy Issues

- Authentication
 - ▣ Are you who you say you are? GFIPM, FICAM, PKI, X.509,...
- Information Privacy Marking
 - ▣ Who should be allowed to access this information? ACLs, IC-ISM, Privacy Annotation
- Information Protection
 - ▣ How to limit non-authorized access to information? XML-Enc, EME, DRM
- Information Integrity
 - ▣ How to verify information hasn't changes? Hash Digests, Digital Signatures
- Information Access/Modification Non-repudiation
 - ▣ How to track access and changes to information? Audit Logs, Digital Signatures
- Information Access/Authorization Policy
 - ▣ What rules apply to authorizing access or changes to information? SAML, XACML
- Information Access/Authorization Negotiation
 - ▣ Is this user allowed to see/change this information given all of the above? GFIPM, FICAM, BAE

One small piece of a much larger privacy and security solution set.

REQUIREMENTS: XML Privacy Annotation

- Fine-resolution XML Annotation & Subsequent Physical Marking
 - ▣ Entire document to individual element
- No impact if not used
 - ▣ Element PrivacyAttributeGroup or IDREF linked PrivacyMetadata
- Simple
 - ▣ Minimum “classification” and “custodian” attributes
- Sophisticated
 - ▣ Classification: full compartmentalized marking
 - ▣ Authorization: allowedAction, releasableTo, restrictedFrom
 - ▣ Policy References: privacy, obligation, delegation, refrain, purpose
 - ▣ annotatedBy : serial (history) and parallel (trump), consent
 - ▣ Expiration: future-proof, especially agency assigned annotations

Privacy Annotation PrivacyAttributeGroup/PrivacyMetadata modeled on IC-ISM Information Security Marking Schema

Privacy

- ☐ custodian
- ☐ classification
- ☐ sensitivity
- ☐ domain
- ☐ subdomain
- ☐ compartment

Policy References

(As Intended When Annotated)

- ☐ privacyPolicy
- ☐ obligationPolicy
- ☐ delegationPolicy
- ☐ refrainPolicy
- ☐ purposePolicy

Annotated By

(Revisions/Multiple Annotations)

- ☐ annotatedBy
- ☐ annotationDateTime
- ☐ reason
- ☐ derivedFrom
- ☐ derivativelyAnnotatedBy
- ☐ consentDocument

Authorization

(Guidance When Annotated)

- ☐ allowedAction
- ☐ displayTo
- ☐ releasableTo
- ☐ restrictedFrom
- ☐ accessNotificationTo

Expiration

- ☐ expirationDateTime
- ☐ expirationEvent
- ☐ expirationException
- ☐ expirationPolicy

PrivacyMetadata Element

```
<xsd:complexType name="PrivacyMetadataType">
  <xsd:complexContent>
    <xsd:extension base="s:MetadataType">
      <xsd:attribute ref="classification" use="required"/>
      <xsd:attribute ref="sensitivity" use="required"/>
      <xsd:attribute ref="compartment" use="optional"/>
      <xsd:attribute ref="custodian" use="required"/>
      <xsd:attribute ref="domain" use="optional"/>
      <xsd:attribute ref="subdomain" use="optional"/>
      <xsd:attribute ref="allowedAction" use="optional"/>
      <xsd:attribute ref="displayTo" use="optional"/>
      <xsd:attribute ref="releasableTo" use="optional"/>
      <xsd:attribute ref="restrictedFrom" use="optional"/>
      <xsd:attribute ref="accessNotificationTo" use="optional"/>
    </xsd:extension>
  </xsd:complexContent>
</xsd:complexType>
```

Classification

Authorization

```
<xsd:attribute ref="privacyPolicy" use="optional"/>
<xsd:attribute ref="obligationPolicy" use="optional"/>
<xsd:attribute ref="delegationPolicy" use="optional"/>
<xsd:attribute ref="refrainPolicy" use="optional"/>
<xsd:attribute ref="purposePolicy" use="optional"/>
<xsd:attribute ref="annotatedBy" use="optional"/>
<xsd:attribute ref="annotationDateTime" use="optional"/>
<xsd:attribute ref="reason" use="optional"/>
<xsd:attribute ref="derivedFrom" use="optional"/>
<xsd:attribute ref="derivativelyAnnotatedBy" use="optional"/>
<xsd:attribute ref="consentDocument" use="optional"/>
<xsd:attribute ref="expirationDateTime" use="optional"/>
<xsd:attribute ref="expirationEvent" use="optional"/>
<xsd:attribute ref="expirationException" use="optional"/>
<xsd:attribute ref="expirationPolicy" use="optional"/>
</xsd:extension>
</xsd:complexContent>
</xsd:complexType>
```

Policies

Annotated By

Expiration

Privacy Annotation Usage

- Annotate w/PrivacyAttributeGroup or IDREF linked PrivacyMetadata
 - ▣ Gross to fine-grain application of annotation
 - Document
 - Complex Object
 - Element
 - ▣ Potential reuse of annotation/consent across multiple elements
 - ▣ No impact on XML instance where not used
- Multiple annotation revisions by same annotatedBy
 - ▣ Supports annotation revision history where required
- Multiple independent annotations (different annotatedBy)
 - ▣ Supports “trump annotations” by higher authority/classification
 - ▣ Subordinate annotations allow fallback if trump removed

Simple Example

....

```
<pi:PersonAssociatesAndLocations>
  <nc:Person s:id="ID_1">
    <nc:PersonName>
      <nc:PersonFullName>
        Ms. Cindy Lu Who
      </nc:PersonFullName>
    </nc:PersonName>
  </nc:Person>
  <nc:Location s:id="ID_2" s:ref="PRIVID_3">
    <nc:LocationAddress>
      <nc:AddressFullText>
        23 Suess Lane, Whoville
      </nc:AddressFullText>
    </nc:LocationAddress>
  </nc:Location>
```

....

```
<privacy:PrivacyMetadata s:id="PRIVID_3">
  <privacy:classification>GREEN</privacy:classification>
  <privacy:custodian>cindy@lu.net</privacy:custodian>
  <privacy:domain>PERSONAL</privacy:domain>
</privacy:privacyMetadata>
```

....

Multiple Marks Example

```
<pi:PersonAssociatesAndLocations>
  <nc:Person sid="ID_1">
    <nc:PersonName>
      <nc:PersonFullName>
        Ms. Cindy Lu Who
      </nc:PersonFullName>
    </nc:PersonName>
  </nc:Person>
  <nc:Location sid="ID_2" s:ref="PRIVID_3 PRIVID_4 PRIVID_5">
    <nc:LocationAddress>
      <nc:AddressFullText>
        23 Suess Lane, Whoville
      </nc:AddressFullText>
    </nc:LocationAddress>
  </nc:Location>
  ....

```

```
<privacy:PrivacyMetadata sid="PRIVID_3">
  <privacy:classification>GREEN</privacy:classification>
  <privacy:custodian>cindy@lu.net</privacy:custodian>
  <privacy:domain>PERSONAL</privacy:domain>
  <privacy:AnnotatedBy>Cindy Lu Who</privacy:AnnotatedBy>
  <privacy:AnnotatedDateTime>2012-02-02T00:00:00</privacy:AnnotatedDateTime>
</ privacy:PrivacyMetadata>

```

Mark 1

```
< privacy:PrivacyMetadata sid="PRIVID_4">
  <privacy:classification>AMBER</privacy:classification>
  <privacy:custodian>cindy@lu.net</privacy:custodian>
  <privacy:domain>PERSONAL</privacy:domain>
  <privacy:AnnotatedBy>Cindy Lu Who</privacy:AnnotatedBy>
  <privacy:AnnotatedDateTime>2013-07-09T15:29:00</privacy:AnnotatedDateTime>
</ privacy:PrivacyMetadata>

```

Mark 2

```
< privacy:PrivacyMetadata sid="PRIVID_5">
  <privacy:classification>RED</privacy:classification>
  <privacy:custodian>connections@ocfs.ny.gov</privacy:custodian>
  <privacy:domain>CYFS</privacy:domain>
  <privacy:compartment>BULLYING</privacy:compartment>
  <privacy:restrictedFrom>Grinch@grrr.com</privacy:restrictedFrom>
</ privacy:PrivacyMetadata>

```

Mark 3

Summary – Privacy Annotation

- Modest proposal
- Simple extension to existing information exchange standards
- Modeled after Intelligence Information Security Marking schema
- Leverages stringent healthcare privacy and policy definitions
- Complimentary to existing privacy and security standards
- Dependent upon full suite of privacy and security services:
 - Policies
 - Rules
 - Consent
 - Authentication
 - Groups/Roles
 - Authorization
 - Encryption
 - etc.

Contact



Brian D. Handspicker

Consulting Architect/Manager

PracticalMarkets, Inc.

413-672-8210

bd@practicalmarkets.net