Conveying data element privacy attributes during information exchange
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**
  - Medical 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 Lack Information Privacy Support

- **HIPAA**
  - HL7 Data Segmentation for Privacy (DS4P)
  - ONC S&I DS4P pilot

- **FERPA**
  - PESC
  - Ed-Fi

- **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 Marking

- **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 Marking

- **Fine-resolution Marking**
  - Entire document to individual element

- **No impact if not used**
  - Mark PrivacyAttributesGroup or IDREF linked PrivacyMetadata

- **Simple**
  - Minimum “classification” and “custodian” attributes

- **Sophisticated**
  - Classification: full compartmentalized marking
  - Authorization: disseminationCode, releasableTo, restrictedFrom
  - Policy References: privacy, obligation, delegation, refrain, purpose
  - MarkedBy: serial (history) and parallel (trump) marking, consent
  - Expiration: future-proof, especially agency assigned marks
Privacy Marking PrivacyAttributesGroup modeled on IC-ISM SecurityAttributesGroup

<table>
<thead>
<tr>
<th>Privacy</th>
<th>Policy References</th>
<th>Marked By</th>
</tr>
</thead>
<tbody>
<tr>
<td>custodian</td>
<td>privacyPolicyReference</td>
<td>markedBy</td>
</tr>
<tr>
<td>classification</td>
<td>obligationPolicyReference</td>
<td>markedDate</td>
</tr>
<tr>
<td>sensitivity</td>
<td>delegationPolicyReference</td>
<td>reason</td>
</tr>
<tr>
<td>domain</td>
<td>refrainPolicyReference</td>
<td>derivedFrom</td>
</tr>
<tr>
<td>subdomain</td>
<td>purposePolicyReference</td>
<td>derivativelymarkedBy</td>
</tr>
<tr>
<td>compartment</td>
<td></td>
<td>consentReference</td>
</tr>
</tbody>
</table>

Authorization

(Guidance When Marked)

- disseminationCode
- displayTo
- releasableTo
- restrictedFrom
- accessNotificationTo

Expiration

- expiryDate
- expiryEvent
- expiryException
- expirationPolicyReference
PrivacyMetadata

<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="disseminationCode" 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:attribute ref="privacyPolicyReference" use="optional"/>
      <xsd:attribute ref="obligationPolicyReference" use="optional"/>
      <xsd:attribute ref="delegationPolicyReference" use="optional"/>
      <xsd:attribute ref="refrainPolicyReference" use="optional"/>
      <xsd:attribute ref="purposePolicyReference" use="optional"/>
      <xsd:attribute ref="markedBy" use="optional"/>
      <xsd:attribute ref="markedDate" use="optional"/>
      <xsd:attribute ref="reason" use="optional"/>
      <xsd:attribute ref="derivedFrom" use="optional"/>
      <xsd:attribute ref="derivativelymarkedBy" use="optional"/>
      <xsd:attribute ref="consentReference" use="optional"/>
      <xsd:attribute ref="expiryDate" use="optional"/>
      <xsd:attribute ref="expiryEvent" use="optional"/>
      <xsd:attribute ref="expiryException" use="optional"/>
      <xsd:attribute ref="expirationPolicyReference" use="optional"/>
    </xsd:extension>
  </xsd:complexContent>
</xsd:complexType>
Mark Usage

- Mark PrivacyAttributesGroup or IDREF linked Metadata
  - Gross to fine-grain application of mark
    - Document
    - Complex Object
    - Element
  - Potential reuse of mark/consent across multiple elements
  - No impact on XML instance where not used

- Multiple mark revisions by same markedBy
  - Supports mark revision history where required

- Multiple independent marks (different markedBy)
  - Supports “trump marks” by higher authority/classification
  - Subordinate marks allow fallback if trump removed
Summary – Privacy Marking

- 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, LLC
413-652-5029
bd@handspicker.net
Informal Examples

If you see the following slides, please note these examples were created for business owners to explain the general concepts. They do not conform to the schema:

- English strings not URI references
- Informal dates not ISO dates
- Etc.
Simple Example

....

<p PessoaAssociatesAndLocations>
  <p Pessoa s:id="ID_1">
    <p PersonName>
      <p PersonFullName>
        Ms. Cindy Lu Who
      </p PersonFullName>
    </p PersonName>
  </p Pessoa>
</p Pessoa>

<p Pessoa s:id="ID_2" s:ref="ID_3">
  <p LocationAddress>
    <p AddressFullText>
      23 Suess Lane, Whoville
    </p AddressFullText>
  </p LocationAddress>
</p Location>

....

<privacy:PrivacyMetadata s:id="ID_3">
  <privacy:classification>GREEN</privacy:classification>
  <privacy:custodian>SELF</privacy:custodian>
  <privacy:domain>PERSONAL</privacy:domain>
</privacy:PrivacyMetadata>

....
Multiple Marks Example

<!-- Mark 1 --><pi:PersonAssociatesAndLocations>
<nc:Person s:id="ID_1">
  <nc:PersonName>
  </nc:PersonName>
  <nc:PersonFullName>
    Ms. Cindy Lu Who
  </nc:PersonFullName>
</nc:Person>
<nc:Location s:id="ID_2" s:ref="ID_3 ID_4 ID_5">
  <nc:LocationAddress>
    <nc:AddressFullText>
      23 Suess Lane, Whoville
    </nc:AddressFullText>
  </nc:LocationAddress>
</nc:Location>

<!-- Mark 2 --><privacy:PrivacyMetadata s:id="ID_3">
  <privacy:classification>GREEN</privacy:classification>
  <privacy:custodian>SELF</privacy:custodian>
  <privacy:domain>PERSONAL</privacy:domain>
  <privacy:markedBy>Cindy Lu Who</privacy:markedBy>
  <privacy:markedDate>01/01/1970</privacy:markedDate>
</privacy:privacyAttributeGroup>
<privacy:PrivacyMetadata s:id="ID_4">
  <privacy:classification>AMBER</privacy:classification>
  <privacy:custodian>SELF</privacy:custodian>
  <privacy:domain>PERSONAL</privacy:domain>
  <privacy:markedBy>Cindy Lu Who</privacy:markedBy>
  <privacy:markedDate>07/14/1973</privacy:markedDate>
</privacy:privacyAttributeGroup>
<privacy:PrivacyMetadata s:id="ID_5">
  <privacy:classification>RED</privacy:classification>
  <privacy:custodian>OCFS</privacy:custodian>
  <privacy:domain>CYFS</privacy:domain>
  <privacy:compartment>BULLYING</privacy:compartment>
  <privacy:restrictedFrom>Grinch</privacy:restrictedFrom>
</privacy:privacyAttributeGroup>

<!-- Mark 3 -->