~~From:~~ **~~Gary Dickinson~~** ~~gary.dickinson@ehr-standards.com~~
~~Subject:~~
~~Date:~~ ~~3 June 2014 at 10:17~~
~~To:~~

~~Begin forwarded message:~~

From: "Kathleen Connor [SRS]" <klc@securityrs.com>
Subject: FHIR Provenance Resource
Date: 1 May 2014 at 12:57:13 PDT
To: Robert Dieterle <rdieterle@enablecare.us>, "Reed Gelzer (r.gelzer@myfairpoint.net)" <r.gelzer@myfairpoint.net>, "Gary Dickinson (gary.dickinson@ehr-standards.com)" <gary.dickinson@ehr-standards.com>, "Walter.g.suarez@kp.org" <Walter.g.suarez@kp.org>, "Ioana Singureanu (ioana.singureanu@gmail.com)" <ioana.singureanu@gmail.com>, "neelimaj70@gmail.com" <neelimaj70@gmail.com>, Bob Yencha <bobyencha@maine.rr.com>, "Johnathan Coleman [SRS]" <jc@securityrs.com>, "Rita Torkzadeh (rtorkzadeh@jbsinternational.com)" <rtorkzadeh@jbsinternational.com>

Hi

RE Lifecycle/lifespan, integrity, and digital signature topics raised in the charter review:

If you haven't had a chance, take a look at the FHIR Provenance Resource (Also, see Provence Resource Definitions)

It's a healthcare profile on W3C PROV and has a digital signature, but for limited use.

The initiative may want to consider recommending the addition of other types of digital signature and integrity mechanisms (attestation, binding of provenance to the target, and non-repudiation).

FHIR Provenance Resource supports lifecycle and lifespan to some extent – hopefully Reed and Gary can review for completeness.

Since FHIR is DSTU, we can make comments recommending changes to FHIR Provenance Resource, which FHIR would likely have to consider as they prepare for normative ballot in January (which means we'd have to have comments submitted by October.)

-K

6.6 Resource Provenance - Content

Provenance information that describes the activity that led to the creation of a set of resources. This information can be used to help determine their reliability or trace where the information in them came from. The focus of the provenance resource is record keeping, audit and traceability, and not explicit statements of clinical significance.

6.6.1 Scope and Usage

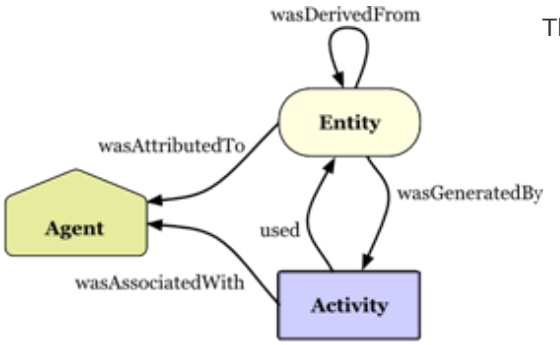
The provenance resource tracks information about activity that created a version of a resource, including the entities, and agents involved in producing a resource. This information can be used to form assessments about its quality, reliability or trustworthiness, or to provide pointers for where to go to further investigate the origins of the resource and the information in it.

Provenance resources are a record-keeping assertion that gathers information about the context in which the information in a resource was obtained. Provenance resources are prepared by the application that initiates the create/update etc. of the resource. A Security Event resource contains overlapping

information, but is created as events occur, to track and audit the events. Security Event resources are often (though not exclusively) created by the application responding to the read/query/create/update etc. event.

6.6.2 Background and Context

The provenance resource is based on the W3C Provenance specification, and mappings are provided. The Provenance resource is tailored to fit the FHIR use-cases for provenance more directly. The W3C Provenance Specification has the following fundamental model:



The *Provenance* resource actually corresponds to a single activity that identifies a set of resources (*target*) generated by the activity. The activity also references other entities (*entity*) that were used and the agents (*agent*) that were associated with the activity.

6.6.3 Resource Content

Provenance (Resource)target : Resource(Any) 1..*period : Period 0..1recorded : instant 1..1reason : CodeableConcept 0..1location : Resource(Location) 0..1policy : uri 0..*integritySignature : string 0..1Agentrole : Coding 1..1 <<ProvenanceAgentRole>>type : Coding 1..1 <<ProvenanceAgentType>>reference : uri 1..1display : string 0..1Entityrole : code 1..1 <<ProvenanceEntityRole>>type : Coding 1..1 <<ProvenanceEntityType>>reference : uri 1..1display : string 0..1agent0..*agent0..1entity0..*

```
<Provenance xmlns="http://hl7.org/fhir">

 <!-- from Resource: extension, modifierExtension, language, text, and contained -->
 <target><!-- 1..* Resource(Any) Target resource(s) (usually version specific) --></target>
 <period><!-- 0..1 Period When the activity occurred --></period>
 <recorded value="[instant]"/><!-- 1..1 When the activity was recorded / updated -->
 <reason><!-- 0..1 CodeableConcept Reason the activity is occurring --></reason>
 <location><!-- 0..1 Resource(Location) Where the activity occurred, if relevant --></location>
 <policy value="[uri]"/><!-- 0..* Policy or plan the activity was defined by -->
 <agent>  <!-- 0..* Person, organization, records, etc. involved in creating resource -->
  <role><!-- 1..1 Coding e.g. author | overseer | enterer | attester | source | cc: + --></role>
  <type><!-- 1..1 Coding e.g. Resource | Person | Application | Record | Document + --></type>
  <reference value="[uri]"/><!-- 1..1 Identity of agent (urn or url) -->
  <display value="[string]"/><!-- 0..1 Human description of participant -->
 </agent>
 <entity>  <!-- 0..* An entity used in this activity -->
  <role value="[code]"/><!-- 1..1 derivation | revision | quotation | source -->
```

```
  <type><!-- 1..1 Coding Resource Type, or something else --></type>
  <reference value="[uri]"/><!-- 1..1 Identity of participant (urn or url) -->
  <display value="[string]"/><!-- 0..1 Human description of participant -->
  <agent><!-- 0..1 Content as for Provenance.agent Entity is attributed to this agent --></agent>
 </entity>
 <integritySignature value="[string]"/><!-- 0..1 Base64 signature (DigSig) - integrity check -->
</Provenance>
```

Alternate definitions: Schema/Schematron, Resource Profile

6.6.3.1 Terminology Bindings

Path	Definition	Type	Reference
Provenance.agent.role	The role that a provenance agent played	Incomplete	http://hl7.org/fhir/vs/provenance-agent-role
Provenance.agent.type	The type of a provenance agent	Incomplete	http://hl7.org/fhir/vs/provenance-agent-type
Provenance.entity.role	How an entity was used in an activity	Fixed	http://hl7.org/fhir/provenance-entity-role
Provenance.entity.type	The type of an entity used in an activity	Incomplete	http://hl7.org/fhir/vs/resource-types

6.6.3.2 Using the Provenance Resource

The provenance resource identifies information about another resource (the *reference* element). The provenance resource may be used in several different ways:

As part of a document bundle where it identifies the provenance of part or all of the document

On a RESTful system where it keeps track of provenance information relating to resources

When used in a document bundle, the *references* are often not explicitly versioned, but they always implicitly pertain to the version of the resource found in the document. On a RESTful system, the target resource reference should be version specific, but this requires special care: For new resources that need to have a corresponding Provenance resource, the version-specific reference is often not knowable until after the target resource has been updated. This can create an integrity problem for the system - what if the provenance resource cannot be created after the target resource has been updated? To avoid any such integrity problems, the target resource and the provenance resources should be submitted as a pair using a transaction.

6.6.3.3 Digital Signatures

The provenance resource includes an integritySignature element which contains an XML digital signature.

The purpose of the signature is limited to checking cryptographic integrity of the target resource(s); e.g.

detecting whether changes have occurred between the original construction of the resource and the application processing it. In order to make proper use of the signature element, implementation profiles are required to further clarify the obligations around creating and checking the signature.

The following rules apply to digital signature:

The Certificate identifier SHOULD match the identity of an agent (Provenance.agent.reference)

If the signature has an IHE purposeOfSignature property, the value SHALL be "source", OID "1.2.840.10065.1.12", which means "the signature of an automated data source". If the signature does not have a purposeOfSignature property, the signature is still to used for this use

Whether the representation of the Provenance resource is xml or json, the signature is a base64 of the XML signature

The signature is always a signature of the target resource XML representation using a stated canonicalization

The signature is only added to support , and not to represent workflow and clinical aspects of the signing process, or to support non-repudiation.

6.6.3.4 Party References

Because the Provenance resource often refers to parties that are not represented as FHIR resources, Agent and Entity references are allowed to be either references to other resources, or they can refer to other entities that are not FHIR resources.

The code in the *.type* element is used to differentiate between the two: if the code is in the system "http://hl7.org/fhir/resource-types", then the reference is to a resource, and the element *reference* functions exactly the same as in a Resource Reference.

A version specific reference to a FHIR resource on the same server:

```
<agent>
  <type>
    <system value="http://hl7.org/fhir/resource-types"/>
    <code value="Person"/>
  </type>
  <reference value="person/@34/history/3"/>
</agent>
```

In effect, this is the same pattern as a standard resource reference, but the type becomes extensible to allow referencing other kinds of resources.

A reference to a user (a person) not represented by a FHIR resource:

```
<agent>
  <type>
    <system value="http://hl7.org/fhir/provenance-participant-type"/>
    <code value="person"/>
```

```
    </type>
    <reference value="http://acme.com/users/34"/>
  </agent>
```

One subtle issue with the use of the Provenance resource is to differentiate between whether the reference is to the Resource itself, or whether the the reference is to the real world thing that the resource represents, e.g. was it the person involved in the activity, or the record of the person. For Agents, it should be understood that the reference is to the real world thing that the resource represents.

6.6.4 Search Parameters

Search parameters for this resource. The standard parameters also apply. See Searching for more information about searching in REST, messaging, and services.

Name	Type	Description	Paths
_id	token	The logical resource id associated with the resource (must be supported by all servers)	
end	date	End time with inclusive boundary, if not ongoing	Provenance.period.end
location	reference	Where the activity occurred, if relevant	Provenance.location (Location)
party	token	Identity of agent (urn or url)	Provenance.agent.reference
partytype	token	e.g. Resource | Person | Application | Record | Document +	Provenance.agent.type
start	date	Starting time with inclusive boundary	Provenance.period.start
target	reference	Target resource(s) (usually version specific)	Provenance.target (Any)

6.6.6 Resource Provenance - Formal Definitions

Formal definitions for the elements in the Provenance resource.

Provenance	
Definition	Provenance information that describes the activity that led to the creation of a set of resources. This information can be used to help determine their reliability or trace where the information in them came from. The focus of the provenance resource is record keeping, audit and traceability, and not explicit statements of clinical significance.

Control 1..1

Comments Some parties may be duplicated between the target resource and its provenance. For instance, the prescriber is usually (but not always) the author of the prescription resource. This resource is defined with close consideration for W3C Provenance.

Provenance.target

Definition The resource(s) that were generated by the activity described in this resource. A provenance can point to more than one target if multiple resources were created/updated by the same activity.

Control 1..*

Type Resource(Any)

Comments Target references are usually version specific, but may not be, if a version has not been assigned or if the provenance information is part of the set of resources being maintained (i.e. a document). When using the RESTful API, the identity of the resource may not be known (especially not the version specific one); the client may either submit the resource first, and then the provenance, or it may submit both using a single transaction. See the notes on transaction for further discussion.

Provenance.period

Definition The period during which the activity occurred.

Control 0..1

Type Period

Comments The period can be a little arbitrary; where possible, the time should correspond to human assessment of the activity time.

Provenance.recorded

Definition The instant of time at which the activity was recorded.

Control 1..1

Type instant

Comments This can be a little different from the time stamp on the resource if there is a delay between recording the event and updating the provenance and target resource.

Provenance.reason

Definition The reason that the activity was taking place.

Control 0..1

Type CodeableConcept

Provenance.location

Provenance.location

Definition	Where the activity occurred, if relevant.
Control	0..1
Type	Resource(Location)

Provenance.policy

Definition	Policy or plan the activity was defined by. Typically, a single activity may have multiple applicable policy documents, such as patient consent, guarantor funding, etc.
Control	0..*
Type	uri

Provenance.agent

Definition	An agent takes a role in an activity such that the agent can be assigned some degree of responsibility for the activity taking place. An agent can be a person, a piece of software, an inanimate object, an organization, or other entities that may be ascribed responsibility.
Control	0..*
Comments	Several agents may be associated (i.e. has some responsibility for an activity) with an activity and vice-versa.

Provenance.agent.role

Definition	The role that the participant played.
Control	1..1
Binding	ProvenanceAgentRole: (See http://hl7.org/fhir/vs/provenance-agent-role)
Type	Coding

Provenance.agent.type

Definition	The type of the participant.
Control	1..1
Binding	ProvenanceAgentType: (See http://hl7.org/fhir/vs/provenance-agent-type)
Type	Coding
Comments	If the type is "Resource" then the resource itself was the participant. If the type is a type of resource, then the entity identified by the resource is the participant.

Provenance.agent.reference

Definition	Identity of participant. May be a logical or physical uri and maybe absolute or relative.
Control	1..1
Type	uri
Comments	identity may be a reference to a resource or to something else, depending on the type.

Provenance.agent.display

Definition	Human-readable description of the participant.
Control	0..1
Type	string

Provenance.entity

Definition	An entity used in this activity.
Control	0..*

Provenance.entity.role

Definition	How the entity was used during the activity.
Control	1..1
Binding	ProvenanceEntityRole: How an entity was used in an activity (see http://hl7.org/fhir/provenance-entity-role for values)
Type	code

Provenance.entity.type

Definition	The type of the entity. If the entity is a resource, then this is a resource type.
Control	1..1
Binding	ProvenanceEntityType: (See http://hl7.org/fhir/vs/resource-types)
Type	Coding
Comments	If the type is "resource" then the resource itself was the participant. If the type is a type of resource, then the entity identified by the resource is the participant.

Provenance.entity.reference

Definition	Identity of participant. May be a logical or physical uri and maybe absolute or relative.
Control	1..1

Type	uri
Comments	identity may be a reference to a resource or to something else, depending on the type.

Provenance.entity.display

Definition	Human-readable description of the entity.
Control	0..1
Type	string

Provenance.entity.agent

Definition	The entity is attributed to an agent to express the agent's responsibility for that entity, possibly along with other agents. This description can be understood as shorthand for saying that the agent was responsible for the activity which generated the entity.
Control	0..1
Type	See Provenance.agent

Provenance.integritySignature

Definition	A digital signature on the target resource(s). The signature should match a Provenance.agent.reference in the provenance resource. The signature is only added to support checking cryptographic integrity of the resource, and not to represent workflow and clinical aspects of the signing process, or to support non-repudiation.
Control	0..1
Type	string
Comments	Whether the content is XML or JSON, the representation is as a base64 of the XML signature of the resource.

Kathleen Connor
Security Risk Solutions, Inc.
ONC/HHS Contractor
Tel: 360 357 3536

Begin forwarded message:

From: "Kathleen Connor [SRS]" <klc@securityrs.com>
Subject: heads up on Prov requirements
Date: 11 May 2014 at 23:59:09 PDT
To: "Reed Gelzer (r.gelzer@myfairpoint.net)" <r.gelzer@myfairpoint.net>, "Gary Dickinson (gary.dickinson@ehr-standards.com)" <gary.dickinson@ehr-standards.com>, "Patricia Van Dyke (patricia.vandyke@modahealth.com)" <patricia.vandyke@modahealth.com>
Cc: "Ioana Singureanu (ioana.singureanu@gmail.com)" <ioana.singureanu@gmail.com>, "neelimaj70@gmail.com"

<neelimaj70@gmail.com>, Bob Yencha <bobyencha@maine.rr.com>

Hi

Had a chance to discuss the following with Pat on Friday at WGM, so she may be able to add more insight.

I wanted to give you folks a heads up that the DPROV TT is planning to give the community homework to list their requirements to bring forward on the following Monday May 12th call.

These will be input into modeling lifecycle/lifespan classes, associations, and value sets.

Much is already supported in CDA but we want to check whether we need to add more capabilities to support EHR WG requirements [likely] – and of course, those that other community members bring forward.

Since you've already put a lot of thought into this, I think you've got a great starter set for us to get moving on.

These will also be useful for explanatory text in the IG about how these requirements can be represented in CDA.

Hoping that those in EHR WG who are interested can bring a list of the following requirement types.

[Note that this list is a starter set, which can be modified based on what we find:

- Authoritative definition of lifecycle and lifespan
- Document or Entry level Roles – Assigned Author, Assigned Entity, Intended Recipient,
- Way in which Roles participate in Document/Entry– e.g., informant, verifier, reviewer (an es-MD requirement?), attester, data enterer
- Sources – e.g., devices, record entry system, clinical data repository, a PHR, and external EHR or HIE
- Relationship of a CDA document or entry to an "upstream" artifact [direct parent and previous generations]– e.g., derived from, excerpted from, replaces, amends
- Type of upstream artifact – e.g., record entry, externally sourced CDA or message
- Attributes of upstream artifacts – effectiveTime, status
- Roles and participations that must, should, may participate in the upstream artifacts and the relevant participationType and participationFunction codes.

Please think about the difference between (1) the lifecycle of an artifact that isn't substantially changed vs. (2) artifact that is a derivative of or (3) a composition of other documents.

I think we will need to model all 3 slightly differently to fit within CDA parameters – although the key actors/participations with likely be needed for all – what will be different is the relationships between the predecessor and the successor.

-K

Kathleen Connor

Security Risk Solutions, Inc.
ONC/HHS Contractor
Tel: 360 357 3536