

SECURITY WGM Minutes (8th May 2019 WED)

Date:

08 May 2019

Quarters - Q2/Q3/Q4

Minutes approved [2019-06-18 Security WG Agenda/Minutes](#)



i This is to approve minutes via general consent. "You have received the minutes. Are there any corrections to the minutes? (pause) Hearing none, if there are no objections, the minutes are approved as printed."

Goals

Set goals, objectives or some context for this meeting.

Discussion items

Time	Item	Who	Notes
Q2		Trish	Chaired by Trish
	Cross-Paradigm Transformation Project	Matt	<p>See slide deck. Cross Paradigm Security May WGM Update Working with ___ to develop CDA to FHIR use cases and V2 to FHIR to develop use cases GOAL to develop maps for V2 to FHIR and CDA to FHIR to Have not included Provenance yet b/c there is no community consensus on how to include Provenance KC: have they looked at CDA Provenance? Speaker: NO</p> <p>FHIR meta.security mapping challenges:</p> <ul style="list-style-type: none"> • meta.security does not provide structural elements capable of indicating semantic difference between different HCS Security labels. • VS ARV segment provides different fields (e.g. Security Classification (ARV-7) Security Handling Instructions (ARV-8), Restriction Message Location (ARV-9) • FHIR meta.security capacity to indicate different semantics limited to -code and .system attributes (not structural, terminological) <p>Additional FHIR Security Mapping Challenges</p> <ul style="list-style-type: none"> • HCS requires that certain security labels be human readable at the clinical statement level of documentation, e.g., 42 USC Part 2, § 2.231 • ARV-5 segment used for rendered content • No recognizable FHIR solution identified <p>Discussion with John M. and KC re codes in HCS</p>
45	PSAF Vol3 Provenance DAM	Mike Davis	<p>HL7 Provenance Conceptual Model. See presentation HL7 Provenance Conceptual Model 0502 2019 1.1.pptx</p> <p>Plan is to ballot informatively in Sept and normative in Feb is informative is supportive. Top down view hopefully to meet FHIR (bottom up) in middle!</p> <p>A key point is the references to chaining (Prov-O Chaining).</p> <p>The security WG and EHR have been working on relationship models between the provenance in general and what this means in healthcare.</p> <p>Mike Davis</p> <p>See slide deck.</p> <p>Threw out other version of work and started over based on comments.</p> <p>Goal to ballot in January 2020.</p> <p>Domain Analysis Model for Provenance</p> <p>Starts from top down, while FHIR starts from bottom up.</p> <p>SLIDE 1.</p> <p>SLIDE 2: Federation: a group of organizations, countries, regions, etc. that have joined together to form a larger organization or government by agreeing to the federations policy Didn't like this model, so came up with another model. See Figure 3.</p> <p>SLIDE 3. Provenance Store is where the entire history of</p> <p>SLIDE 4: Definitions (see "redirect" in particular)</p>

			<p>SLIDE 5: Provenance Model. Agent sends stuff to recipient. Recipients can request / receive provenance info. Can request from Provenance store....can receive from an agent. Agent can also send REDIRECT to the Store to get it to send Provenance info to the Recipient.</p> <p>SLIDE 6: Broker</p> <p>SLIDE 7: Provenance Entity Use Cases. NB: The Store can do analysis on Provenance chain and identify error sources...</p> <p>SLIDE 8: (slide crossed out)</p> <p>SLIDE 9: Provenance Storyboards: tracking production history, attribution, locate error sources, quality assessment, focused search.... (could have others).</p> <p>SLIDE 10: Federated Provenance Model (slide crossed out)</p> <p>KC, JM, Discussion re: confidence re integrity (e.g. setting levels re: confidence level based on source of information (patient, provider author, assembler, etc.))</p> <p>SLIDE 11: Provenance Services (IBM Watson Paper which echoed what was being ballot)</p> <p>SLIDE 12: (slide crossed out)</p> <p>SLIDE 13: Illustration of trust mechanism put in place by the Federation.</p> <p>SLIDE 14: (slide crossed out) boundary view</p> <p>SLIDE 15: Boundary diagram (current)</p> <p>SLIDE 16: Core Provenance Metadata to be captured:</p> <ul style="list-style-type: none"> • Who contributed to the generation of a CDA • When an information event recorded in a CDA occurred • Where an information event recorded • Why an information event recorded • Chaining (specifically defined) discussion of "lineage"...this version of the DAM does not go into lineage....it stops at "chain"). • What provenance metadata • One more.....see slide <p>SLIDE 17: Prov Events (non-normative)</p> <p>SLIDE 18 (slide crossed out) Lineage</p> <p>SLIDE 19: (slide crossed out) Lineage</p> <p>SLIDE 20: (slide crossed out) Lineage</p> <p>SLIDE 21: Provenance Internal Agent Service Model (Appendix) (right now this is in a non-normative appendix to the DAM, but it is not discussed in any great detail.)</p> <p>SLIDE 22: first effort at Chaining. (slide crossed out)</p> <p>SLIDE 23: second effort (slide cross out)</p> <p>SLIDE 24: Provenance Chaining (Prov-0) Now include "informed by" and "acted on behalf of...." Both concepts are important to chaining.</p> <p>SLIDE 25: (slide cross out)</p> <p>SLIDE 26: Provenance Class Model 1: Base: (Collection is a collection of entities that are treated as ONE entity).</p> <p>SLIDE 27: Data Chaining: (slide cross out)</p> <p>SLIDE 28 (slide cross out)</p> <p>SLIDE 29: Prov-O Chaining (4 types of chains)</p> <ul style="list-style-type: none"> • Activity+Entity chain (<i>used and generated by</i>) • Activity Chain ("<i>was informed by</i>" relationship) • Entity Chain ("<i>as derived from</i>") • Agent Chains ("<i>acted on behalf of</i>") <p>SLIDE 30:</p>
20	V2 to FHIR	Craig Newmann & Matt Lord	<p>Cross Paradigm Transformation Service. Progress report</p> <p>Overview - Use cases and functional specification for transformation services between HL7 models. V2, FHIR, CDA etc.</p> <p>FHIR provenance under consideration but a lack of consensus on how this is handled in FHIR has limited the progress in this to date.</p> <p>FHIR meta.security has mapping challenges. For instance the capacity to indicate different semantic is limited to .code and .system attributes (not structural but terminological). SOA and SEC needs to collaborate further on this. Goal is to work with Security and OO and FHIR-I to find appropriate methods for implementing HCS.</p>
-	DPROV CDA	Kathleen	Deferred

15	Basic Provenance IG	Brett Marquard /Russ Ott	<p>This session was used to discuss what work can we accomplish with the SEC WG to follow up on the project. The project is advanced sufficiently to go to the functional community and ask where to apply the provenance rules. We know the type of content but what circumstances and level does the information need to be recorded? May be useful to present the Prov-O to the community but the concepts/terminology may need to be adjusted to ensure that the terms are used the same.</p> <p>Need support as they communicate with the clinical community. Signup for the call on Mondays, - details listed on SEC list.</p> <p>NEXT STEPS: go to the functional committee and get guidance on where to apply provenance to. Good enough to be at the document level? Does it need to beat the section level? If so, which sections. Does it need to be at the entry level?</p> <p>Need to ID the elements to be used (look to W3C)</p> <p>Need to Cross-walk from the terms they are using (Author, etc) to the terms used in the W3C world.</p> <p>JM: W3C: if something is ACTING then they are agents. If something is acted upon, it's an ENTITY. ROLE is used to distinguish between the various AGENTS:</p> <p>BASIC PROVENANCE focuses on TREATMENT:</p> <p>MIKE's DAM applies broadly...e.g., RESEARCH etc. as well.</p> <p>JM: putting the PROV-O in front of the clinicians may not be a bad thing.....they are concerned about the meta data in the information itself, ORIGINAL INFO v. COPIED INFO, vs DERIVED FROM info, etc.</p> <p>MIKE: there is a lot of provenance in the health record....e.g., record indicates patient said they had an allergy....the PATIENT is the sourcethat is the provenance of the information. The TRUST that the clinician has in the information will reflect the source of the information.</p>
WED Q3			
		Trish	Chaired by Trish
40	Security - PSAF Work Session	Mike David	<p>PSAF Vol 3 Provenance Prep for Sept ballot. Mike went through the changes already made in the document. Document is being kept at a reasonably high level. Fuller descriptions of some concepts has been included. Mike will finish the draft of the document and then send it out to the group for comment and completion of missing sections where more information is requested.</p> <ul style="list-style-type: none"> Data flow sequence diagrams are missing currently, John will complete this. Class models text is a more mature section - all the models established between security and EHR are referred to for comparison. The provenance chaining has specific definitions and have been grouped together in one section. Requirements section needs review. Collated from multiple sources - high level requirements for provenance and may not be useful for implementation but for understanding. <p>Suggestion to send out completed section for comment rather than whole document. Perhaps put it in Confluences as per the development of GDPR white paper.</p>
15	Provenance	Kathleen	<p>Review Data Provenance CDA IG. The DSTU has expired.. There is work going on related to CDA provenance, and renewed interest . So it needs to move forward to normative track or be retired.</p> <p>CBCP is the owner for the project but Security could take it over if CBCP doesn't have an interest or provide support. Check with ONC about interest in supporting.</p> <p>MOTION: We vote to refresh with the caveat of finding out what is the administrative process for this. Asking CBCP to move it forward to normative ballot.</p> <p>Kathleen proposed, Mike seconded. Carried 10:2:0</p>
20	Security FHIR Considerations	John	<p>Resolutions:</p> <p>GF#22104: Provenance.activity needs ISO 21089 vocabulary</p> <p>GF#22103: Need Clarity on Provenance.target use to support findable</p> <p>GF#21646: Need Provenance.activity query parameter posted by john.moehrke</p>
WED Q4			
GDPR Session			
			Chaired by Alex Mense
20	MedMij	Alexander Henket	<ul style="list-style-type: none"> MedMij (pronounced med-my) and other HIT security and privacy, Alexander Henket, NICITZ NL <ul style="list-style-type: none"> video link can be found on YouTube and www.medmij.nl It is focused on giving patients control over their records and collation of these. It contains a trust framework - and contains security aspects. How is GDPR incorporated? It is not overtly incorporated but is assumed that people will follow the regulations. FHIR STU3 based.
25	GDPR FHIR IG	Alex Mense	<p>Finished work on the white paper (available in Confluence) . Security>Projects> FHIR-GDPR.</p> <p>The confluence page has some use cases (based on the patient summary). The next step is to create an implementation guide on how to implement the requirements. Hence we need a new project and PSS.</p> <p>Project scope statement - needs to be generalised to be able to create several artifacts from the PSS. For instance initially include 2 Use Cases. Proposal to write IG covering 5 generic use cases. Alex to draft PSS and circulate for comment.</p>

5	GDPR White Paper update	Alex Mense	Finished work on the white paper (available in Confluence) . Security>Projects> FHIR-GDPR.
5	GDPR Use Cases	Giorgio Cangioli	Will the PSS cover the existing Use Cases on international patient summary and stop this work as a separate item? There was no plan to continue on this use case, as it is currently really supporting information. International Patient Summary: Use Cases
10	GDPR Vocabulary	Peter van Liesdonk	Use case is radiology /oncology, for instance image reuse. Under GDPR this re-use is identified as processing, and therefore there is a requirement under GDPR. Going to need to track purposes in use of information. Security labels could be used.
10	GDPR "Right to Be Forgotten"	Teresa Aardal Connor	GDPR "Right to Be Forgotten" with respect to Health Information - Legal Review. Produced table on how it relates to other national law. Article 23 is the key part for "rights". Collated the corresponding national laws. Specifically Article 9 - permission to be able process PHI without consent. Consideration of not only use, but retaining information to for other legal purposes. The challenge is how to translate this into IGs and security labels and policies. Teresa to provide a synopsis of this. 4.15.2019 DRAFT_comparison of sections subject to national laws.xlsx
10		Peter van Liesdonk	Research with genomic data -open access. But this is personal information so under GDPR you cannot use this data. The issue is the different countries have different consent processes, and GDPR means you need to re-consent.

Action items

