Committee Approval Date:
Security WG approved this FHIR IG Proposal

2020-01-14 Security Agenda/Minutes

Publishing Lead:
Mohammad Jafari/John Moehrke

Contributing or Reviewing Work Groups:
Cosponsor: CBCP WG approved

FHIR Data Segmentation for Privacy (DS4P) Implementation Guide PSS

Jun 04, 2019

FHIR Development Project Insight ID:

Scope of coverage:
Application of FHIR meta.security to segment FHIR Bundles and Resources per applicable policy.

Content location:
FHIR GitHub
Security WG Confluence site - for discussion, draft content, reference material

Proposed IG realm and code:
UV/security-label-ds4p

Maintenance Plan:
HL7 Security WG will provide ongoing support for this IG.

Short Description:
Provides FHIR guidance for applying security labels with coded tags for use in access control systems governing the collection, access, use, and disclosure of the target FHIR Resource(s) as required by applicable organizational, jurisdictional, or personal "sharing with protection" policies.

Long Description:
Provides FHIR guidance on:
• How to select a security label based on the HL7 Privacy and Security Healthcare Classification System (HCS) label adjudication algorithms, the value in establishing consensus on a default security label for representing policies or consent directives within an exchange ecosystem, and the value of establishing default security labels for information exchanged within the Trust Framework of a policy domain.

• How an Access Control System, such as an OAuth Authorization Server can use the security labels to filter responses to person/population based queries and pushed disclosures that meets:
  - Authorization Requirements specifying control over whether or not a client’s request for import or export of person/population Resources will be permitted
  - Filtering Requirements specifying, at a more fine-grained level, what resources will appear in the results of a person/population export or accepted in an import operation, including approaches to filtering for the minimum necessary information based on policy
  - Transformation Requirements specifying the requirements for applying functions on imported or exported person/population Resources, which modify and transform the content of any Resource per applicable privacy/security policies and/or data subject's(s’) consent directive
  - Provenance Requirements specifying the recording and consumption of provenance information in a person/population Resource(s) export or import operation.

Describes how to structure FHIR meta.security to meet the HL7 Healthcare Privacy and Security Classification System syntactic and semantic rules to convey computable and interoperable policy within a policy domain by use of Trust Contracts with binding capability statements.

Describes the use of FHIR meta.security extensions to enable specification of the manner in which security label "privacy marks" are rendered, e.g., per CUI requirements; reference policy, contract, or consent directive instances; indicate the authority responsible for the assigned security label; and indicate whether a label has been upgraded, downgraded, or declassified, and the party responsible for doing so.

Involved parties:

VHA
DOD
Sequoia Project
eHealth Exchange

HIT vendors who exchange information using FHIR that requires or could benefit from the ability to assign computable and interoperable security labels

Expected implementations:

May 16, 2020 - Connectathon Track to demonstrate the FHIR Security Label Examples at May Connectathon as part of a FHIR DS4P Track.

Sept 19, 2020 - Connectathon Track to test transforms and Trust Contract profile

Content sources:


HL7 US Regulatory Security Label IG

Example Scenarios:

How to develop consensus Security Label for a domain policy, including privacy, security, patient, or trust based on algorithm for parsing policy requirements per HCS.

How a custodian or sender determines whether a Resource needs a specific Security Label.

How a sender determines the High-Water Mark security label on a Bundle when (1) all bundled Resources have the same security labels; (2) when bundled Resources have different or no security labels.

How as receiver appropriately handles Bundle and Resource labels.

Develop Trust Contracts with capability statements about:

• A sender's ability to determine the correct security labels to assign to Resources and to the Bundle as the High-Water Mark.
• A receiver's ability to consume, persist, enforce, display security labels as required.

How a sender determines whether a receiver is capable of consuming, persisting, enforcing, and displaying security labels using Trust Contract capability statements.

IG Relationships:

FHIR DS4P provides the profile upon which the FHIR US Regulatory Security Label IG is based.

Timelines:
January 2020 - Draft CUI, Part2, and 7332 Security Labels examples based on FHIR DS4P; V2.9 FHS, BHS, MSH, and ARV; and DS4P CDA IG. Draft use cases, policy background, and explanatory text.

February 2020 - Vet and refine examples and text with domain and business experts for adherence to policy and implementability.

March 2020 - Develop Cross Paradigm IG based on the examples and text in appropriate syntax.

March 1, 2020 - Submit May NIB for FHIR Security Label IG STU 1 ballot

April 5, 2020 - Final content

May 16, 2020 - Connectathon Track to demonstrate the FHIR Security Label Examples at May Connectathon as part of a FHIR DS4P Track.

June 2020 - Reconcile IG

July 2020 - Revise per reconciliation. Develop transform mappings between security label syntaxes and FHIR Trust Contract with capability statements indicating which security labels are supported.

July 5, 2020 - Submit NIB for FHIR Security Label IG with FHIR Security Label Trust Contract and Transforms across syntaxes for STU 2 ballot

July 21, 2020 - Submit Sept Connectathon track proposal to demonstrate FHIR Security Labels with FHIR Security Label Trust Contract and Transforms across syntaxes

July 28, 2020 - Reconciliation deadline

July 28, 2020 - FHIR Ballot Freeze

August 9, 2020 - Final content deadline

Sept 14, 2020 - Begin Reconciliation

Sept 19, 2020 - Connectathon Track to test transforms and Trust Contract profile

October 2020 - Finalize IG content per reconciliation and request publication

FMG Notes

- Approved 2020-01-15 FMG Agenda/Minutes