Use of Security Labels in FHIR

Proposal for HL7 Belgium WG Infrastructure & Security

Version management

Version	Date	Description	Author
0.1	12/09/2022	First analysis	Brecht Van Vooren
0.2	13/09/2022	Update after VAZG feedback	Brecht Van Vooren
0.3	27/06/2023	Update after feedback José	Brecht Van Vooren

1. General

As applications we store FHIR resources in scope of different projects and with different types of sensitive and privacy content.

Different resource types will be used for specific business use cases. Some resource types will be used by different projects and/or actors. In some cases it may be required to separate access based on the scope of the resource.

2. Security in FHIR

FHIR is not a security protocol, but we do need security when transferring patients data. The FHIR documentation made a summary on the security protocols it can be used with: https://hl7.org/fhir/security.html#6.1.0.

For this document let's focus on Authorization / Access Control and Labels.

"Authorization/Access Control - FHIR defines a Security Label infrastructure to support access control management. FHIR may also define a set of resources to administer access control management, but does not define any at present"

"Labels - FHIR allows for set of security related tags that affect the way resources are handled"

3. Security Labels

In the FHIR docs (https://hl7.org/fhir/security-labels.html), the following is described about security labels:

"A security label is a concept attached to a resource or bundle that provides specific security metadata about the information it is fixed to."

"A security label is represented as a Coding, with the following important properties: system, code, display."

"The Access Control decision engine uses the security label together with any provenance resources associated with the resource and other metadata (e.g. the resource type, resource contents, etc.) to

- approve read, change, and other operations
- determine what resources can be returned
- determine what handling caveats must be conveyed with the data"

"The intent of a security label is that the recipient of resources or bundles with security-tags is obligated to enforce the handling caveats of the tags and carry the security labels forward as appropriate."

4. Proposal

For this proposal we are not enforcing any choice in matter of the decision engine. We want to standardize the usage of the Security Label to literally label a resource to a certain scope, business domain, business owner, … .

By doing this it makes it possible to distinguish different scoped resources that are standardized by the same FHIR profile.

Security Labels offer an easy solution, without the need to declare a linked resource (that can be lost).

5. Use cases

5.1. Existing use cases

UC1: Careplan integrated care vs careplan Population screening:

The careplan that is used for population screening has a completely different context and meaning then the careplan that is used for integrated care:

- Other expectations towards visualization
- Other expectations towards testing/interop
- Other expectations towards access of enduser

UC2: Communication integrated care vs communication population screening vs communication patient summary:

The communication for integrated care is meant in the context of the integrated careplanning and limited to the careteam.

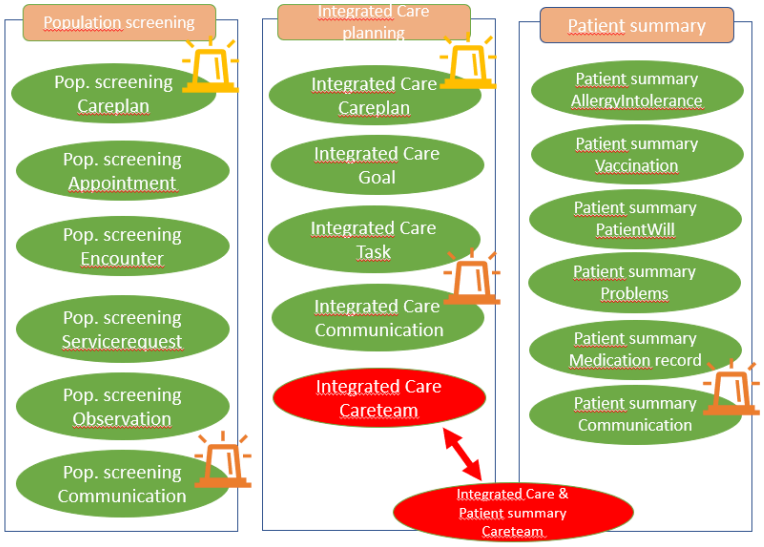
The communication for population screening gives extra information about the population screening results and follow-up

The communication for patient summary *could* give minimal information for patient summary for interdisciplinary acute care (Beware: this is a currently fictitious but not unthinkable example)

5.2. Possible evolution

We should also consider evolving expectations.

UC3: The integrated care careteam could become a careteam that is relevant in the context of the patient summary for interdisciplinary acute care. (Beware: This is a currently fictitious but not unthinkable example)



We need to define a CodeSystem/ValueSet with allowed security labels in the Belgian context.

Example

```
{
  "id": "1",
  "meta": {
    "security": [{
        "system": "https://www.ehealth.fgov.be/standards/fhir/core/CodeSystem/be-securitylabel ",
        "code": "PATIENT_SUMMARY",
        "display": "Patient Summary"
      }]
  }
}
```