Advancing SDOH Interoperability: Enabling Privacy and Consent through Standards and Implementations

Part 1 – Status of Standards Relevant to Supporting SDOH Data Exchange

May 24, 2021

The Office of the National Coordinator for
Health Information Technology

Meeting Etiquette

- Attendees are muted by default. Please keep your phone on mute.
- This webinar is being recorded and will be made available at the Advancing SDOH Health IT Enabled Tools and Data Interoperability Confluence site: https://oncprojectracking.healthit.gov/wiki/display/ASHIETDI/Advancing+SDoH+Health+IT+Enabled+Tools+and+Data+Interoperability+Home
- The slide deck is accessible under the handouts section of the GoToWebinar widget. It will also be made available at the Confluence site above.
- Use the “Questions” feature for your questions and comments
  - We will be moderating and addressing them at the end of the webinar during the Q&A portion

Agenda

Topic	Presenter
Opening Remarks	Elisabeth Myers & Ryan Argentieri, Office of the National Coordinator (ONC)
Overview	Amber Patel, Security Risk Solutions, Inc.
Security Tags and the ONC Final Rule / Data Tagging in Standards	Johnathan Coleman, Security Risk Solutions, Inc.
SMARTv2	Josh Mandel, Chief Architect for SMART Health IT & Microsoft Healthcare
Data Segmentation for Privacy (DS4P) FHIR Implementation Guide	Kathleen Connor, HL7 Security WG Co-chair
USCDI Security Labels Data Elements	Kathleen Connor, HL7 Security WG Co-chair
HEART Standard	Nancy Lush, Patient Centric Solutions
HL7 SDOH Clinical Care Implementation Guide	Bob Dieterle, Technical Director, Gravity Project
Q&A	

Opening Remarks

Elisabeth Myers & Ryan Argentieri

ONC

Overview

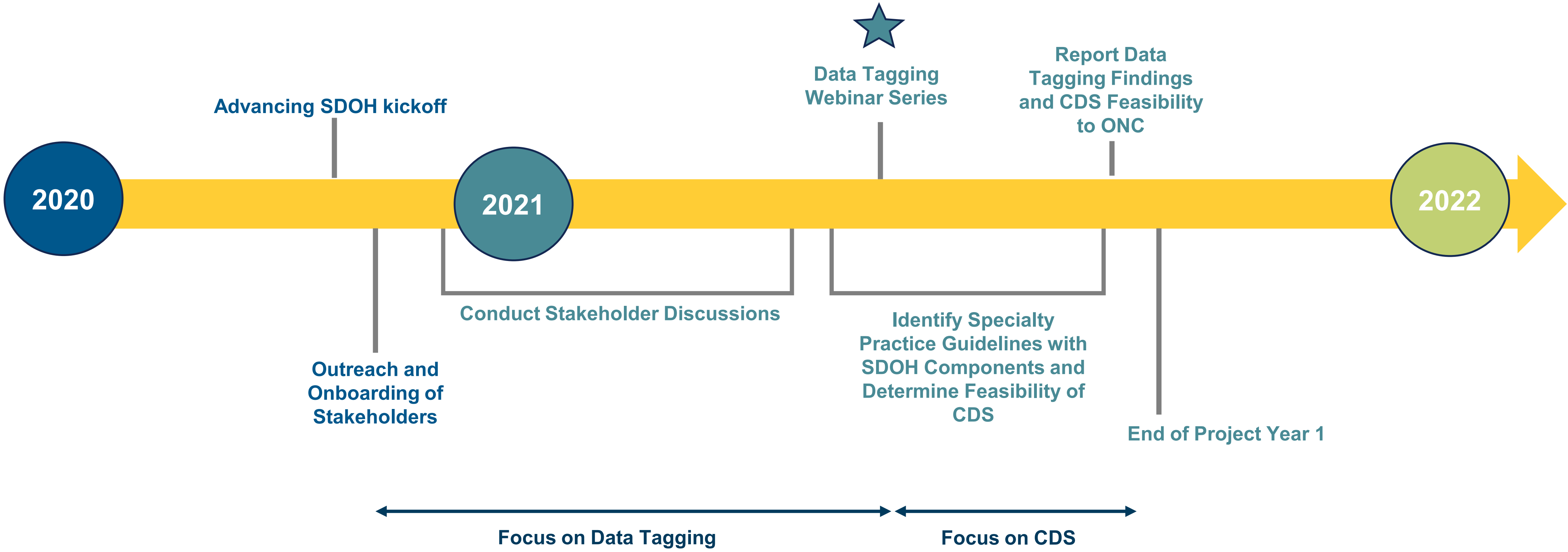
Amber Patel, LL.M.

Security Risk Solutions, Inc.

The Office of the National Coordinator for Health Information Technology

ONC’s Advancing SDOH Health IT Enabled Tools and Data Interoperability Project

- **Scope**: Advance the interoperability of SDOH data by supporting stakeholder led efforts to conduct *data tagging* and to determine the feasibility of developing *clinical decision support* (CDS) for SDOH



2020

Advancing SDOH kickoff

Outreach and Onboarding of Stakeholders

2021

Conduct Stakeholder Discussions

Data Tagging Webinar Series

Identify Specialty Practice Guidelines with SDOH Components and Determine Feasibility of CDS

Report Data Tagging Findings and CDS Feasibility to ONC

End of Project Year 1

2022

Focus on Data Tagging

Focus on CDS

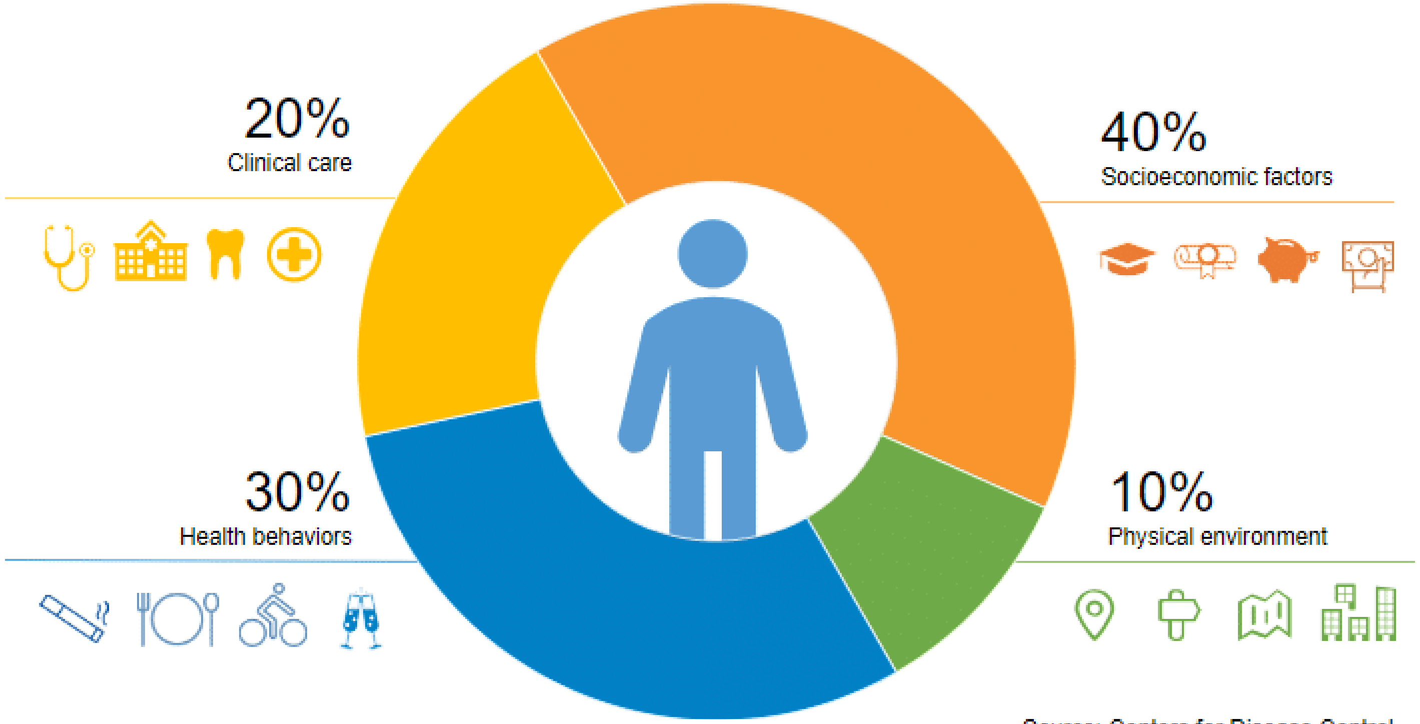
Advancing SDOH Interoperability Webinar Series

- **Part 1** Status of standards relevant to supporting SDOH data exchange through enabling privacy protections, the capture of patient consent, and data tagging
- **Part 2** will take place on **Wednesday, June 2, from 2:00 – 3:00pm ET**, and will feature presentations from organizations working to leverage, test, and implement the standards discussed in Part 1. Please join us by registering here: https://attendee.gotowebinar.com/register/1339137407889722894

The Importance of SDOH Interoperability

- Up to 80% of a person's health is determined by social factors

"When I was a family doctor and a patient would tell me about a need that our organization didn't address – such as housing instability, food insecurity, or transportation challenges – often I would look something up quickly on the internet and then scribble the number of some kind of service on a yellow sticky note"
- Jacob Reider, MD, CEO of the Alliance for Better Health



Source: Centers for Disease Control

Security Tags and the ONC Final Rule

Johnathan Coleman, CISSP, CISM, CRISC

Principal, Security Risk Solutions, Inc.

The Office of the National Coordinator for
Health Information Technology

Security Tags and the ONC Final Rule*

21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program

- The rule implements certain provisions of the 21st Century Cures Act, including Conditions and Maintenance of Certification requirements for health IT developers under the ONC Health IT Certification Program, and necessary activities that do not constitute information blocking.
- The rule also finalizes certain modifications to the 2015 Edition health IT certification criteria and Program in additional ways to advance interoperability, enhance health IT certification, and reduce burden and costs.

*Federal Register: 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program

Security Tags and the ONC Final Rule

Changes from the 2015 Edition Final Rule:

In this final rule, ONC changed the names of the two current 2015 Edition DS4P criteria:

- §170.315(b)(7) Data segmentation for privacy- send, which was used for creating a summary record according to the DS4P standard, changed to

  §170.315(b)(7) Security tags - summary of care – send

- §170.315(b)(8) Data segmentation for privacy – receive, which was used for receiving a summary record according to the DS4P standard, changed to

  §170.315(b)(8) Security tags - summary of care - receive

Security Tags and the ONC Final Rule

Changes from the 2015 Edition Final Rule:

- Certification to the 2015 Edition DS4P criteria only required security tagging of Consolidated-Clinical Document Architecture (C-CDA) documents ***at the document level***, and certification to these criteria was not linked to meeting the Certified EHR Technology definition (CEHRT) used in CMS programs.

- Based on public comment, industry field testing, public forums, listening sessions, and correspondence, ONC updated the requirements for these criteria to support security tagging ***at the document, section, and entry levels***.

- This change better reflects the purpose of these criteria and enables adopters to support a more granular approach to security tagging clinical documents for exchange.

Security Tags and the ONC Final Rule

Regulation Text: §170.315 (b)(7) Security tags – summary of care – send.

Enable a user to create a summary record formatted in accordance with the standard adopted in § 170.205(a)(4)* that is tagged as restricted and subject to restrictions on re-disclosure according to the standard adopted in § 170.205(o)(1)** at the:

(i) Document, section, and entry (data element) level; or

(ii) Document level for the period until December 31, 2022.

* § 170.205(a)(4) - HL7 Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes (US Realm)

** § 170.205(o)(1) - HL7 Version 3 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1, Part 1: CDA R2 and Privacy Metadata Reusable Content Profile

Security Tags and the ONC Final Rule

Regulation Text: §170.315 (b)(8) Security tags – summary of care – receive.

(i) Enable a user to receive a summary record that is formatted in accordance with the standard adopted in § 170.205(a)(4)* that is tagged as restricted and subject to restrictions on re-disclosure according to the standard adopted in § 170.205(o)(1)** at the:

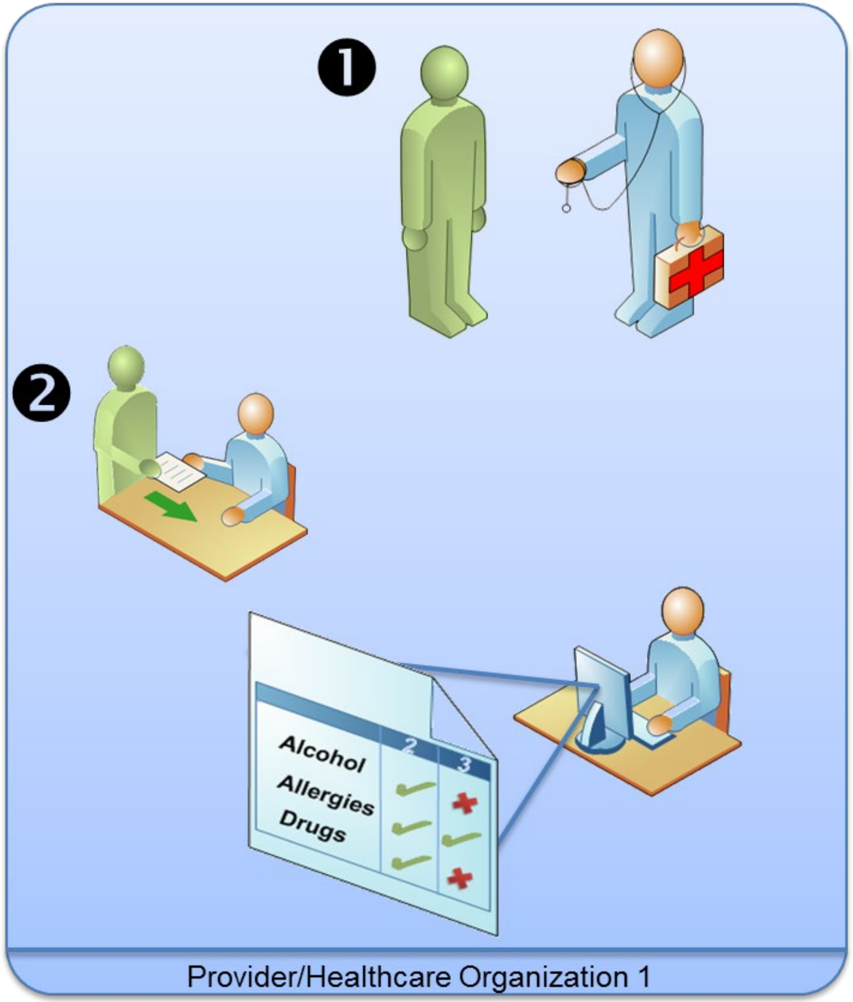
(A) Document, section, and entry (data element) level; or
(B) Document level for the period until December 31, 2022; and

(ii) Preserve privacy markings to ensure fidelity to the tagging based on consent and with respect to sharing and re-disclosure restrictions.

* § 170.205(a)(4) - HL7 Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes (US Realm)

** § 170.205(o)(1) - HL7 Version 3 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1, Part 1: CDA R2 and Privacy Metadata Reusable Content Profile

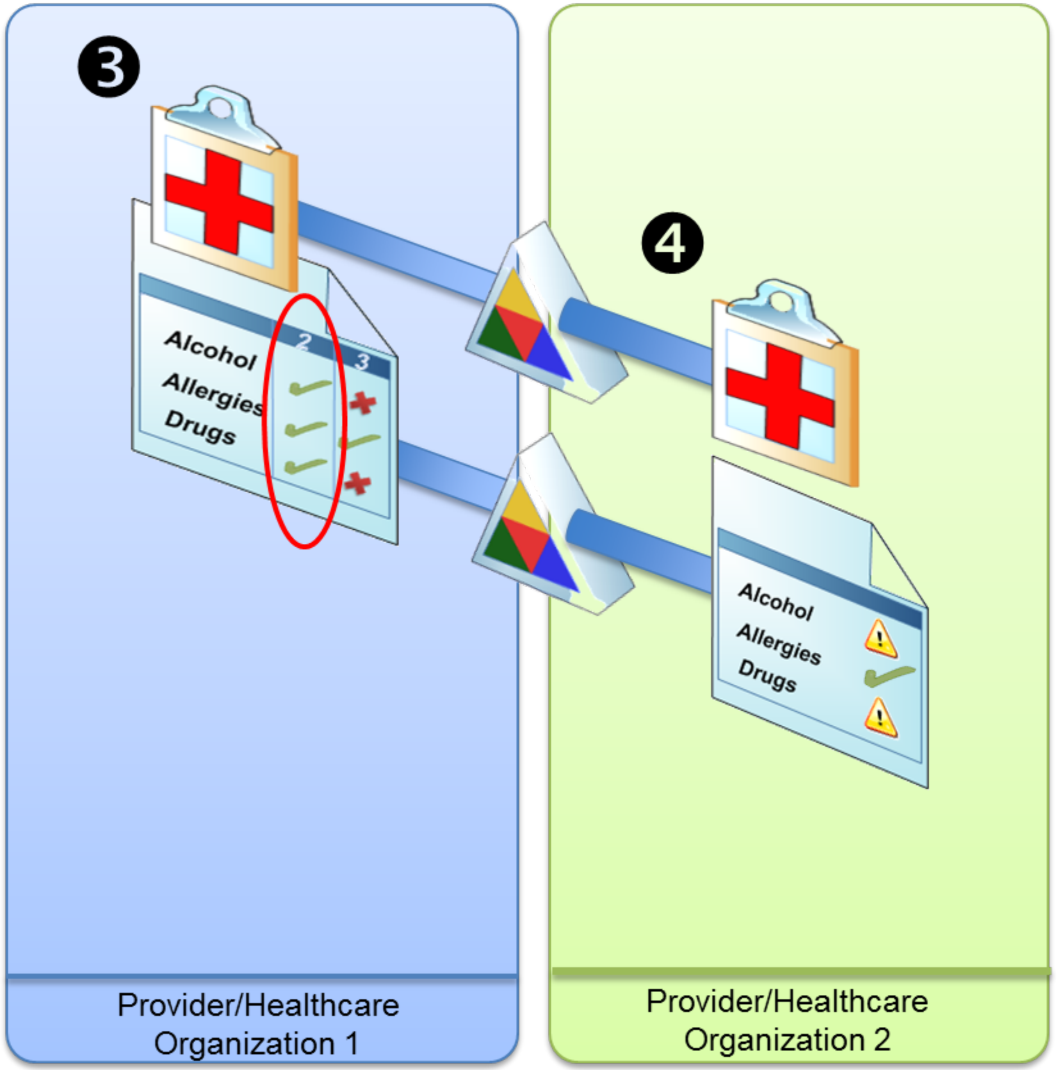
Data Tagging in Standards – Simplified Use Case



❶ A Patient receives care at their local hospital for a variety of conditions, including substance misuse as part of an Alcohol/Drug Abuse Treatment Program.

❷ Data requiring additional protection (and consent, if applicable) are captured and recorded. The patient specified that certain protected information shall not be shared without their consent.

Data Tagging in Standards – Simplified Use Case


❸
Alcohol
Allergies
Drugs
2
3
❹
Alcohol
Allergies
Drugs
Provider/Healthcare Organization 1
Provider/Healthcare Organization 2

❸ The patient now needs data to be sent to an external organization. This disclosure has been authorized by the patient, so the data requiring heightened protection is sent along with a prohibition on redisclosure.

❹ The external organization electronically receives and incorporates all the data, including the protected data, along with any annotations, and the prohibition on redisclosure.

DS4P Vocabularies

DS4P uses vocabularies to convey specific meanings, such as “Do not re-disclose without consent” or “This document is restricted”

STANDARD: HL7 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1 (Includes Content Profile, Profile for Direct, Profile for exchange)		
Capability	**Standards/Profiles used by the HL7 DS4P R1 Standard**	**Specific Usage**
Metadata Vocabularies (for Transport and/or Document Metadata)	***HL7 BasicConfidentialityCodeKind***	Used to represent confidentiality codes associated with disclosed health information (e.g. restricted) as specified in the HL7 Healthcare Security Classification standard (HCS)
	HL7 RefrainPolicy	Conveys specific prohibitions on the use of disclosed health information (e.g. prohibition of redisclosure without consent)
	HL7 PurposeofUse	Conveys the purpose of the disclosure of health information (e.g. treatment, research, emergency)
	HL7 ObligationCode	Used to convey specific obligations associated with disclosed health information (e.g. encryption)
	HL7 ActPolicyType	Used to convey a type of policy
	HL7 SensitivityPrivacyPolicy	Used to convey the sensitivity level of a specific policy

Thanks!

Coming up next…

SMARTv2 (Josh Mandel)

Data Segmentation for Privacy (DS4P) FHIR Implementation Guide (Kathleen Connor)

USCDI Security Labels (Kathleen Connor)

HEART standard (Nancy Lush)

HL7 SDOH Clinical Care Implementation Guide (Bob Dieterle)

Data Tagging in Support in Standards SMARTv2

Josh Mandel, MD

Chief Architect for SMART Health IT and Microsoft Healthcare

The Office of the National Coordinator for
Health Information Technology

Data Segmentation for Privacy (DS4P) FHIR IG

How to develop SDOH Security Labels

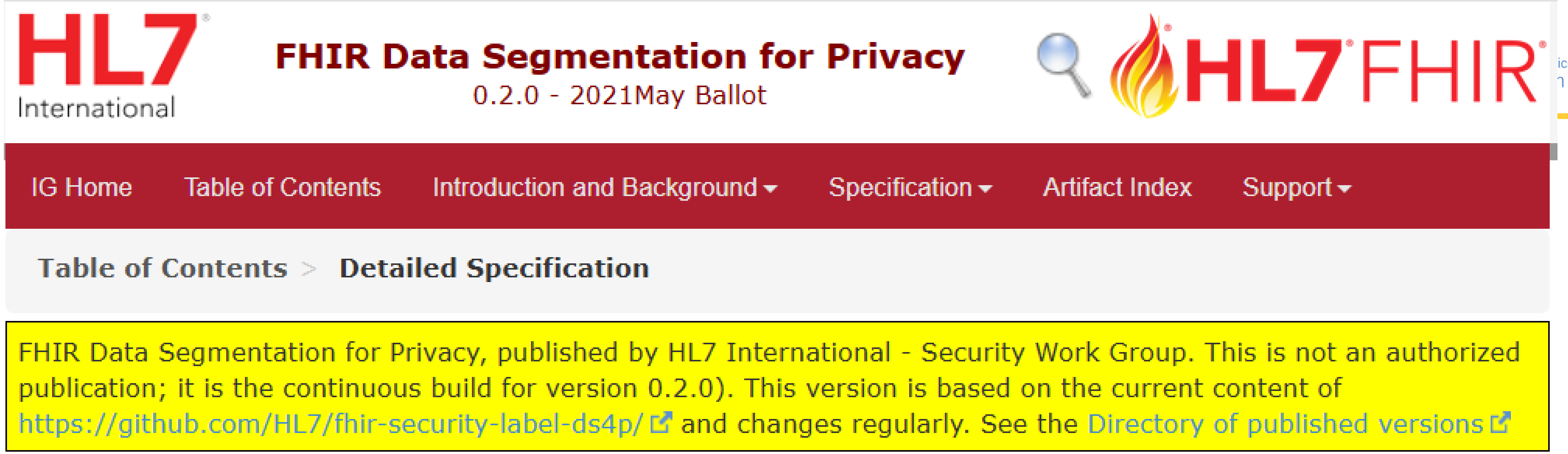
Kathleen Connor MPA

HL7 Security Work Group Co-chair

The Office of the National Coordinator for Health Information Technology

Agenda

- Given the short presentation time, the focus is on the FHIR Data Segmentation for Privacy (DS4P) Implementation Guide (IG)
- Assuming familiarity with the basics of Security Labeling, Data Segmentation policies, technologies, and standards
- Security Labeling Overview and Resources are available at the end of this deck
- Basic Idea – Security Labels are like these Icons on the products we buy – used on health information *shared with protection*



FHIR Data Segmentation for Privacy

0.2.0 - 2021May Ballot

Table of Contents > Detailed Specification

FHIR Data Segmentation for Privacy, published by HL7 International - Security Work Group. This is not an authorized publication; it is the continuous build for version 0.2.0). This version is based on the current content of https://github.com/HL7/fhir-security-label-ds4p/ and changes regularly. See the Directory of published versions

This 2nd STU Ballot provides guidance for using Security Labels for Segmentation* in FHIR, which explains:

- How FHIR Resource.meta.security can emulate the syntactical structure for security labeling defined in the HL7 Healthcare Privacy and Security Classification System (HCS)

- Use in Access Control Systems governing the collection, access, use, and disclosure of FHIR Resource(s) as required by applicable organizational, jurisdictional, or personal *“Share with Protection"* policies.

❖ **Segmentation** The process of sequestering from capture, access or view certain data elements or “datatypes” (clinical information categories) that are perceived by a legal entity, institution, organization, or individual as being undesirable to share.

Basis of FHIR Security Labels is the HCS

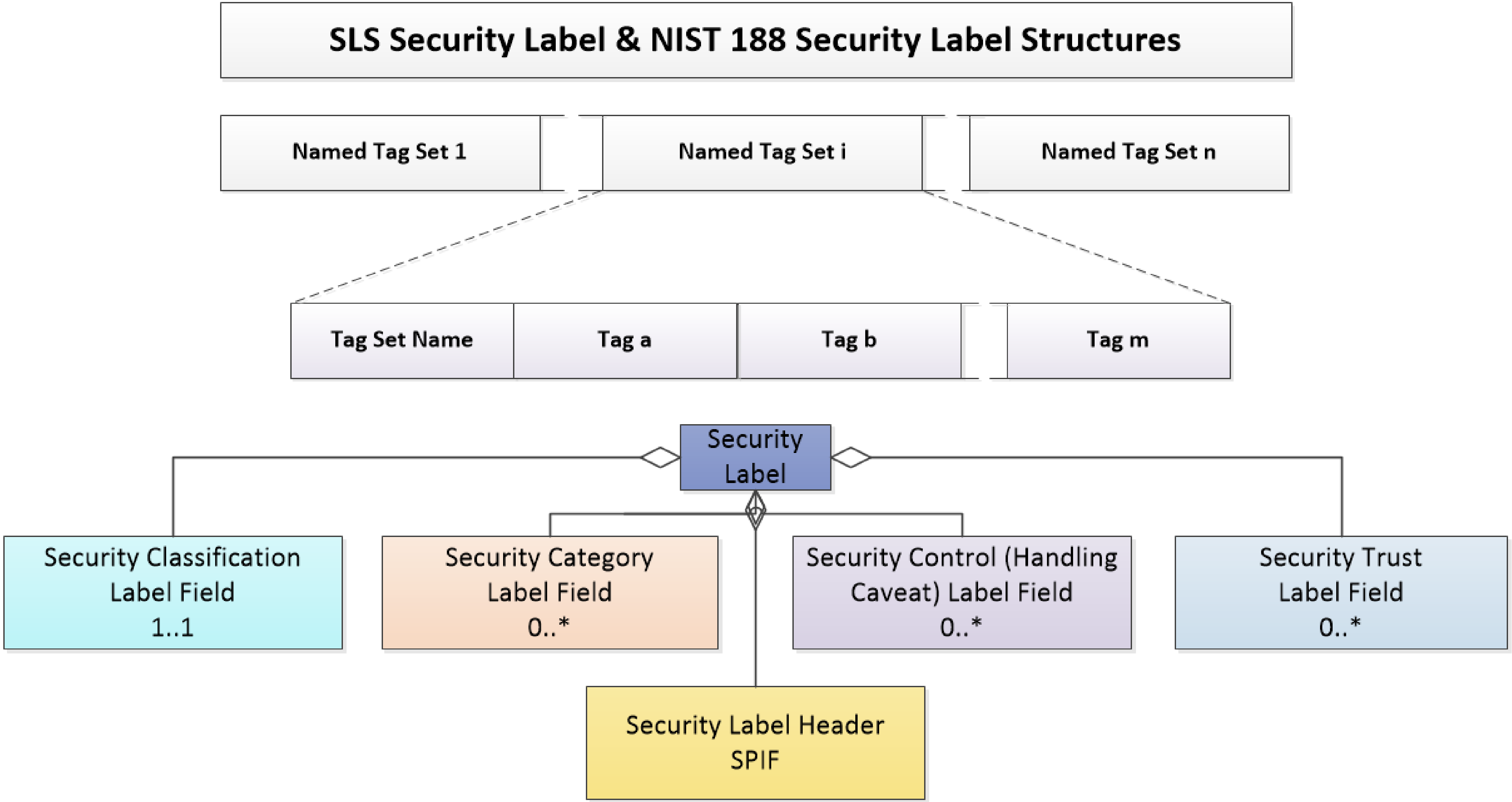
The HL7 HCS is the normative, conceptual model upon which HL7 Version 2.9, the HL7 Implementation Guide: Data Segmentation for Privacy (DS4P) and the HL7 CDA® R2 Implementation Guide: Data Provenance are based.

HCS is healthcare's version of the Security Labels used by the Intelligence Community such as "Top Secret", "Secret", "NOFORN", "Limited Dissemination" codes, which restrict access to End Users with a "Need to Know".

It is based on Foundational Security Standards, NIST specifications, and DOD Directives

HCS syntax structures Security Labels, which dictates how HL7 Security Labeling terminology is used to populate specific fields or "Named Tag Sets" in a security label with appropriate "Security Label Tags" in order to represent a computable policy.

HCS Security Label Syntax Model - High Level



SLS Security Label & NIST 188 Security Label Structures
Named Tag Set 1
Named Tag Set i
Named Tag Set n
Tag Set Name
Tag a
Tag b
Tag m
Security Label
Security Classification Label Field 1..1
Security Category Label Field 0..*
Security Control (Handling Caveat) Label Field 0..*
Security Trust Label Field 0..*
Security Label Header SPIF

Why FHIR DS4P IG?

While all are based on HCS, each HL7 interoperability Product Family – V2, V3, CDA, and FHIR – structures label syntax differently.

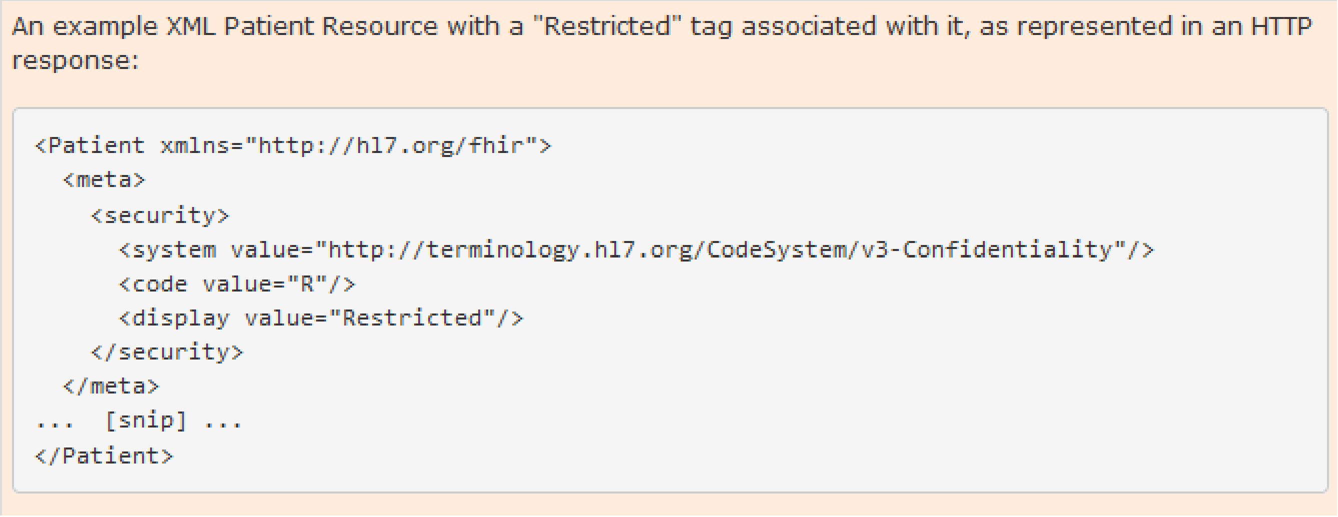
FHIR Core Resource.meta has security label elements that are not specifically HCS conformant.

FHIR Resource.meta.security is simply a list of security label tags - See Security Labels.

Without guidance, any policy could be conveyed differently, which would not be interoperable or easily enforceable with Access Control Systems.

A security label is represented as a Coding, with the following important properties:

system	The coding scheme from which label is taken (see code system URI, and below)
code	a code from the coding scheme that identifies the security label and code is a value from the code system
display	The display form for the code (mostly for use when a system doesn't recognize the code)



An example XML Patient Resource with a "Restricted" tag associated with it, as represented in an HTTP response:

```
<Patient xmlns="http://hl7.org/fhir">
  <meta>
    <security>
      <system value="http://terminology.hl7.org/CodeSystem/v3-Confidentiality"/>
      <code value="R"/>
      <display value="Restricted"/>
    </security>
  </meta>
...  [snip] ...
</Patient>
```

FHIR Security Label Extensions

FHIR DS4P IG explains how to structure FHIR Resource.meta.security to emulate the syntax for security labeling defined in the HCS using 6 extensions, which specify:

- Label’s Policy Basis – e.g., a privacy law
- Label’s Classifier – e.g., a provider, patient, or HIE
- Label’s Related Artifacts – e.g., Provenance, Policy citation, or Consent Directive
- What must be displayed to End Users – e.g., DRAFT, CONFIDENTIAL, Do Not Redisclose, and Controlled Unclassified Information (CUI)

In addition to labeling a Resource/Bundle, the FHIR DS4P IG supports Granular Segmentation at the sub-resource level, which specify:

- Resource has inline label – e.g., a sensitive contained Resource, which cannot include a label in its meta
- Inline Label – e.g., a sensitive identifier such as SSN

sec-label-basis Extension

The Office of the National Coordinator for Health Information Technology

Extension Structure Definition	Description	JSON Snippet	Examples	Usage Notes

Structure definition for the extension-sec-label-basis extension	Enables specifying the policy or regulation based on which a label has been assigned.
	The need: In HCS, the key/value pairs in a Security Label are called Named Tag Sets/Tag Sets and the values are Tags. A Security Label instance represents applicable policy as a specified set of Named Tag Sets/Tag Sets with applicable Tag values.
	This pattern is followed explicitly in HL7 V2.9 and DS4P CDA IG. In FHIR, there's no differentiation between Named Tag Sets/Tag Sets, so there is no built-in way to delineate the <security> elements belonging to a specific policy.
	In order to address, the FHIR DS4P IG specifies the use of extension-sec-label-basis on each <security> within a group of <security> elements belonging to a specific policy.
		{
		"resourceType" : "Observation",
		"id" : "example-extension-sec-label-basis",
		"meta" : {
		"security" : [
		{
		"extension" : [
		{
		"url" : "http://hl7.org/fhir/uv/security-label-ds4p/StructureDefinition/extension-sec-label-basis",
		"valueCoding" : {
		"system" : "http://terminology.hl7.org/CodeSystem/v3-ActCode",
		"code" : "42CFRPart2"
		}
		}
		],
		"system" : "http://terminology.hl7.org/CodeSystem/v3-Confidentiality",
		"code" : "R",
		"display" : "Restricted"
		}
		]
		},
		"text" : {
		"status" : "generated",
		"div" : "<div xmlns=\"http://www.w3.org/1999/xhtml\"><p><b>Generated Narrative</b></p><p></p><p><b>code</b>: <span title=\"Codes: {http://loinc.org 600-7}\">Bacteria identified in Blood by Culture</span></p><p><b>subject</b>: <a href=\"Patient-P001.html\">Generated Summary: active</a></p></div>"
		},
		"status" : "final",
		"code" : {
		"coding" : [
		{
		"system" : "http://loinc.org",
		"code" : "600-7",
		"display" : "Bacteria identified in Blood by Culture"
		}
		]
		},
		"subject" : {
		"reference" : "Patient/P001"
		}
		}
			For example, if a federal agency labels a Resource as 42 CFR Part 2 information, then the Resource would have both Part 2 and CUI security labels in the meta. As a result, all the Part 2 security labels would have a sec-label-basis extension indicating that the basis for the label is Part 2, and all the CUI security labels would have a sec-label-basis indicating that the basis for the label is CFR 32 Part 2002.	This extension SHALL be used on a security label (i.e., in the context of Resource.meta.security) if there is only one policy being conveyed by the all of the security label elements in meta. When more than one policy is conveyed by the security label elements in meta, this extension SHALL be used with each security label element used to convey a specific policy.

sec-label-classifier Extension

Extension Structure Definition	Description	JSON Snippet	Examples	Usage Notes

Structure definition for the extension-sec-label-classifier extension	Enables recording the entity that has assigned or updated the label.	{
		"resourceType" : "Observation",
		"id" : "example-extension-sec-label-classifier",
		"meta" : {
		"security" : [
		{
		"extension" : [
		{
		"url" : "http://hl7.org/fhir/uv/security-label-ds4p/StructureDefinition/extension-sec-label-classifier",
		"valueContributor" : {
		"type" : "reviewer",
		"name" : "John Doe",
		"contact" : [
		{
		"name" : "John Doe",
		"telecom" : [
		{
		"system" : "email",
		"value" : "john@doe.com",
		"use" : "work"
		}
		]
		}
		]
		}
		}
		],
		"system" : "http://terminology.hl7.org/CodeSystem/v3-Confidentiality",
		"code" : "R",
		"display" : "Restricted"
		}
		]
		}
			Use cases for changing security labels include: Permitting more or less restrictive confidentiality level protection, e.g., in the US, from normal under HIPAA to moderate once released via an Individual Right of Access Directive.
			For example, if a patient discloses a HIPAA governed Resource to a non-HIPAA covered entity, that Resource is no longer protected at the level of HIPAA, which is the “norm” for protection in the US. The patient disclosed information would be protected under laws that are different from the norm, and are typically less protective. So, the confidentiality label would be downgraded from normal to moderate.
			The entity downgrading the patient disclosed information may or may not be the patient. It could be done by the disclosing Covered Entity or a third party App based on the patient’s Right of Access Directive.
				This extension SHOULD be used on a security label (i.e., in the context of Resource.meta.security) so that the type, name, and contact information for the contributor of a security label can be identified and retrieved.
				For example, the security label codes may originally be assigned by a classifier authority or agent. Later, the security label code may be reclassified with a different code when the governing policy of a Resource changes.
				The ability to convey the authority or agent name, contact, and classification role may be required by classification policies within a domain.

sec-label-related-artifact Extension

Extension Structure Definition	Description	JSON Snippet	Examples	Usage Notes

Structure definition for the extension-sec-label-related-artifact extension	Enables recording a pointer to an artifact related to the label, particularly, a consent directive based on which the label has been assigned, or a provenance resource which further backs up the integrity label.	{
		"resourceType" : "Observation",
		"id" : "example-extension-sec-label-related-artifact-consent",
		"meta" : {
		"security" : [
		{
		"extension" : [
		{
		"url" : "http://hl7.org/fhir/uv/security-label-ds4p/StructureDefinition/extension-sec-label-related-artifact",
		"valueRelatedArtifact" : {
		"type" : "justification",
		"url" : "http://example.fhir.org/base/Consent/218304"
		}
		}
		],
		"system" : "http://terminology.hl7.org/CodeSystem/v3-Confidentiality",
		"code" : "R",
		"display" : "Restricted"
		}
		]
		},
		"text" : {
		"status" : "generated",
		"div" : "<div xmlns=\"http://www.w3.org/1999/xhtml\"><p><b>Generated Narrative</b></p><p></p><p><b>code</b>: <span title=\"Codes: {http://loinc.org 600-7}\">Bacteria identified in Blood by Culture</span></p><p><b>subject</b>: <a href=\"Patient-P001.html\">Generated Summary: active</a></p></div>"
		},
		"status" : "final",
		"code" : {
		"coding" : [
		{
		"system" : "http://loinc.org",
		"code" : "600-7",
		"display" : "Bacteria identified in Blood by Culture"
		}
		]
		},
		"subject" : {
		"reference" : "Patient/P001"
		}
		}
			Examples include a policy security label code, which is justified based on a law, patient consent directive, or organizational policy; a provenance security label, which is documented by a Provenance Resource; a trust security label code, which is documented by a trust accreditation certificate, trust mark, or a trust agreement such as a DURSA.	This extension SHOULD be used on a security label code for which justification or documentation can be found in an attached or discoverable information instance

must-display Extension

Extension Structure Definition	Description	JSON Snippet	Examples	Usage Notes

Structure definition for the must-display extension	Specifies that a marking must be displayed when the resource is rendered in print or in electronic form. May include the author and the markdown role may be required by classification policies within a domain.	{
		"resourceType" : "Patient",
		"id" : "P001",
		"meta" : {
		"extension" : [
		{
		"url" : "http://hl7.org/fhir/uv/security-label-ds4p/StructureDefinition/extension-must-display",
		"valueAnnotation" : {
		"authorReference" : {
		"type" : "Organization",
		"display" : "Veteran Health Administration"
		},
		"text" : "**CUI//SP-HLTH/HLTH/PRVCY**\r\n\r\n ([Veterans Health Administration, Washington, DC 20420](http://example.fhir.org/Organization/vha))"
		}
		}
		]
		},
		"text" : {
		"status" : "generated",
		"div" : "<div xmlns=\"http://www.w3.org/1999/xhtml\"><p><b>Generated Narrative</b></p><p><b>active</b>: true</p></div>"
		},
		"active" : true
		}
			The PrivacyMark code for 42 CFR Part 2 Prohibition against redisclosure without consent.
			SecurityLabelMark code for Controlled Unclassified Information (CUI), Confidential, DraftMARK, or CopyMARK
			.
				This extension SHOULD be used in the context of Resource.meta when codes from the PrivacyMark or SecurityLabelMark value sets indicate that certain information is to be rendered to end users.
				The must-display extension supports inclusion of the Annotation's author and contact, and markdown for how the information is to be displayed.

has-inline and inline-sec-label Extensions

Extension Structure Definition	Description	JSON Snippet	Examples	Usage Notes

Structure definition for the has-inline-sec-label extension	Indicates whether a resource contains any inline security labels.	{
		"resourceType": "Patient",
		"meta": {
		"extension": [
		{
		"url": "http://hl7.org/fhir/uv/security-label-ds4p/StructureDefinition/extension-has-inline-sec-label",
		"valueBoolean": true
		}
		],
			Resource with sensitive contained Resource (sensitive lab result), identifier (SSN) or address (Women's Shelter) element.	Assists Resource consumers in deciding whether they should to a deep inspection of the Resource content to look for inline security labels.

Structure definition for the inline-sec-label extension	An element-specific security label appearing inline within the element.	"extension": [
		{
		"url": "http://hl7.org/fhir/uv/security-label-ds4p/StructureDefinition/extension-inline-sec-label",
		"valueCoding": {
		"system": "http://terminology.hl7.org/CodeSystem/v3-Confidentiality",
		"code": "R",
		"display": "restricted"
		}
		}
		],
		"use" : "official",
		"system" : "http://hl7.org/fhir/sid/us-ssn",
		"value" : "111-22-3333“
		},
			Resource elements for contained Sensitive lab result Resource, SSN identifier, or Women's Shelter address.	Enables specifying a security label inline on any element in a resource where an extension is allowed to appear.

Cross Paradigm US Regulatory Security Labeling IG

There is an ongoing need for guidance and examples on how a community, such as that promoting SDoH, can develop consensus Security Labels for specific policies to minimize variance and ensure uniform enforcement among trading partners.

While FHIR DS4P IG is “policy agnostic”, it forms the basis for Policy Specific Labeling Profiles.

The Cross Paradigm US Regulatory Security Labeling IG is an initial set of Policy Specific Labeling Profiles is being developed for HL7 V2, CDA, and FHIR for CUI, 42 CFR Part 2, and other use cases such as:

- Data Withholding Request to Prevent Harm
  - Could be used to specify that lab will not release results by patient request or based on provider's concern of physical harm.
  - Could be used to document Information Blocking Privacy Exemption based on patient request or based on HIPAA Privacy Rule permitting providers to withhold release of information to parents/personal representatives based on concern of physical harm.
- **Protecting Privacy to Promote Interoperability (PP2PI) Clinical Use Cases**
  - Mom/Babe Use Case - Security labels to restrict access/use/disclosure of nursery records containing sensitive maternal information such as substance use and number of pregnancies resulting in live births.

USCDI Security Labels

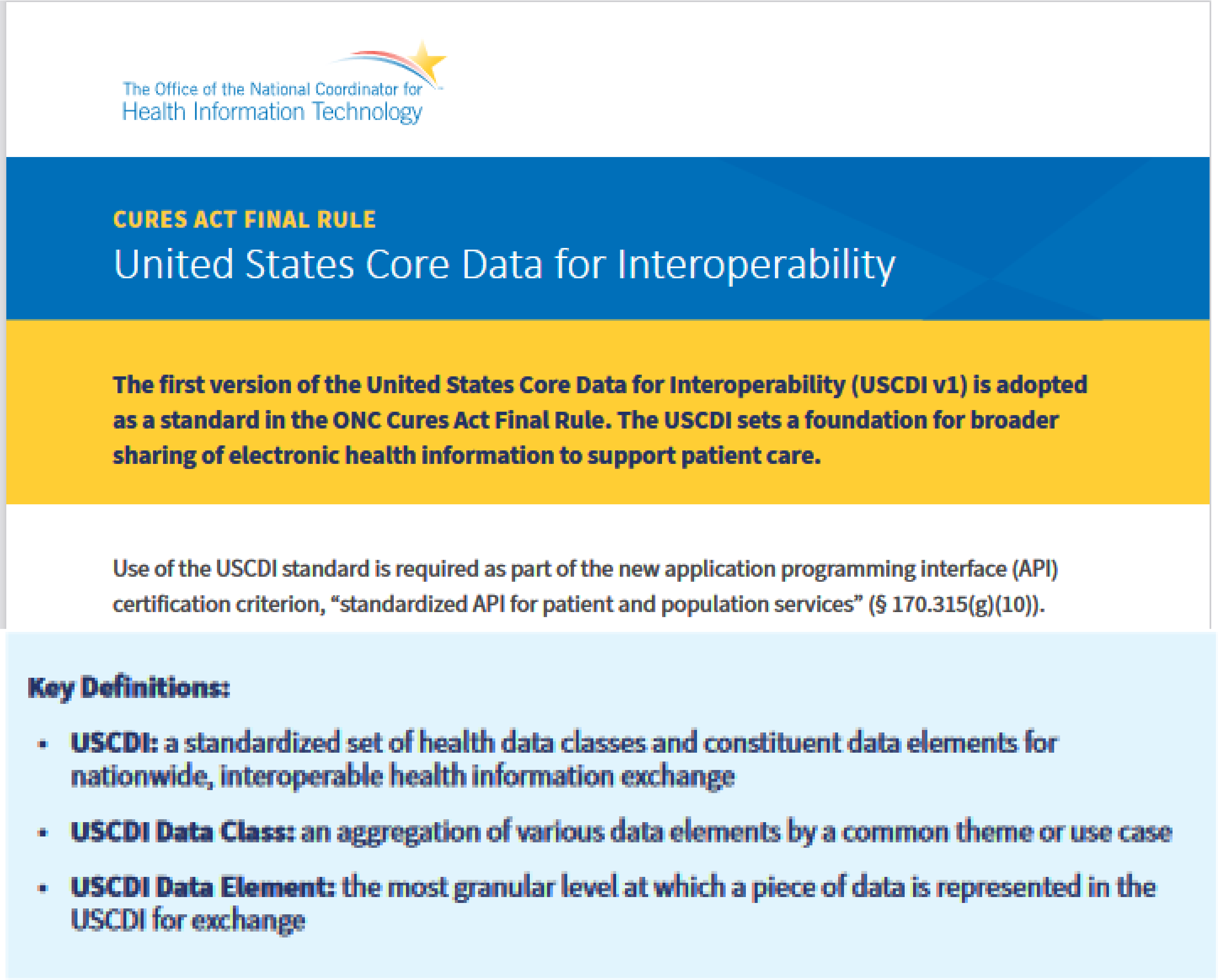
Importance for Protecting SDoH Data

Kathleen Connor MPA
HL7 Security Work Group Cochair

The Office of the National Coordinator for
Health Information Technology

USCDI – What and Why

- The United States Core Data for Interoperability (USCDI) is a standardized set of health data classes and constituent data elements for nationwide, interoperable health information exchange.
- The USCDI ONC New Data Element and Class (ONDEC) Submission System supports a predictable, transparent, and collaborative process, allowing health IT stakeholders to submit new data elements and classes for future versions of USCDI.



The Office of the National Coordinator for Health Information Technology

CURES ACT FINAL RULE

United States Core Data for Interoperability

The first version of the United States Core Data for Interoperability (USCDI v1) is adopted as a standard in the ONC Cures Act Final Rule. The USCDI sets a foundation for broader sharing of electronic health information to support patient care.

Use of the USCDI standard is required as part of the new application programming interface (API) certification criterion, "standardized API for patient and population services" (§ 170.315(g)(10)).

Key Definitions:

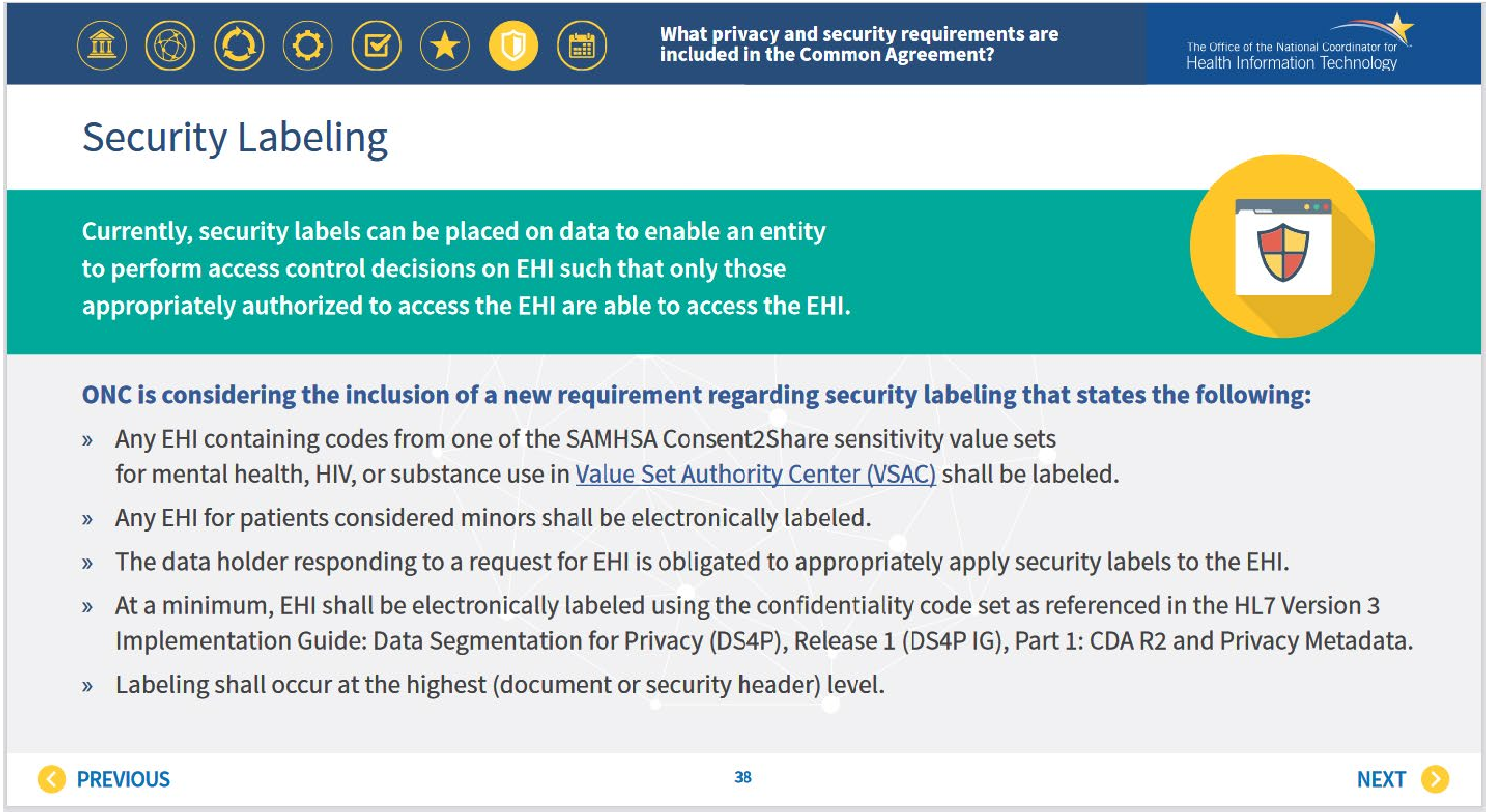
- **USCDI:** a standardized set of health data classes and constituent data elements for nationwide, interoperable health information exchange
- **USCDI Data Class:** an aggregation of various data elements by a common theme or use case
- **USCDI Data Element:** the most granular level at which a piece of data is represented in the USCDI for exchange

Why USCDI Security Labels?

HL7 recommended 6 Security Label Tags as the *minimum starter set* for priority Data Segmentation for Privacy use cases to support development of interoperable, consensus Security Labels for priority policies governing healthcare information mandated to be shared under ONC Cures Rule and CMS Interoperability and Patient Access Final Rule.

Drivers include CURES Rule Granular Segmentation, Draft 2 TEFCA Security Labels, and, increasingly, new USCDI Classes and Elements needing protection including:

- Patient Identifier, Mother's Maiden Name, Gender Identity, Sexual Orientation
- Sensitive Health Concerns, Encounters, Problems, Procedures, Labs, and Medications
- Family History
- Genetics
- Reproductive Health Services
- Social History and Behavioral Health
- Social Determinants of Health (SDoH)



What privacy and security requirements are included in the Common Agreement?

The Office of the National Coordinator for Health Information Technology

Security Labeling

Currently, security labels can be placed on data to enable an entity to perform access control decisions on EHI such that only those appropriately authorized to access the EHI are able to access the EHI.

ONC is considering the inclusion of a new requirement regarding security labeling that states the following:

» Any EHI containing codes from one of the SAMHSA Consent2Share sensitivity value sets for mental health, HIV, or substance use in Value Set Authority Center (VSAC) shall be labeled.

» Any EHI for patients considered minors shall be electronically labeled.

» The data holder responding to a request for EHI is obligated to appropriately apply security labels to the EHI.

» At a minimum, EHI shall be electronically labeled using the confidentiality code set as referenced in the HL7 Version 3 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1 (DS4P IG), Part 1: CDA R2 and Privacy Metadata.

» Labeling shall occur at the highest (document or security header) level.

USCDI Security Labels

Security Labels in USCDI Level 1 Level 1 data elements demonstrate limited existing use in electronic systems, limited exchange between systems and more well-defined use cases and value to potential users. There may still be some burdens associated with development and implementation. Level one bullet

Confidentiality is the 1..1 component of a Security Label that represents the level of protection prescribed by a policy governing the information to which a label is assigned.

- Metadata classifying an IT resource (clinical fact, data, information object, service, or system capability) according to its level of sensitivity, which is based on an analysis of applicable privacy policies and the risk of financial, reputational, or other harm to an individual or entity that could result if made available or disclosed to unauthorized individuals, entities, or processes.

Purpose of Use is the 0..* component of a Security Label that indicates the circumstances under which an authorized recipient is permitted to perform an activity such as create, collect, access, use, or disclose.

- Metadata that segments an IT resource by conveying the reason for performing one or more operations on information, which may be permitted by source system's security policy in accordance with one or more privacy policies and consent directives.

USCDI Security Labels and SDoH

Security Labels in USCDI Comment Level "Comment" level is represented by health care standard terminology such as SNOMED CT® or implementation specifications such as HL7® FHIR® 4. It may not have a well-defined use case or value to potential users. There may be significant or unknown burdens associated with development or implementation.

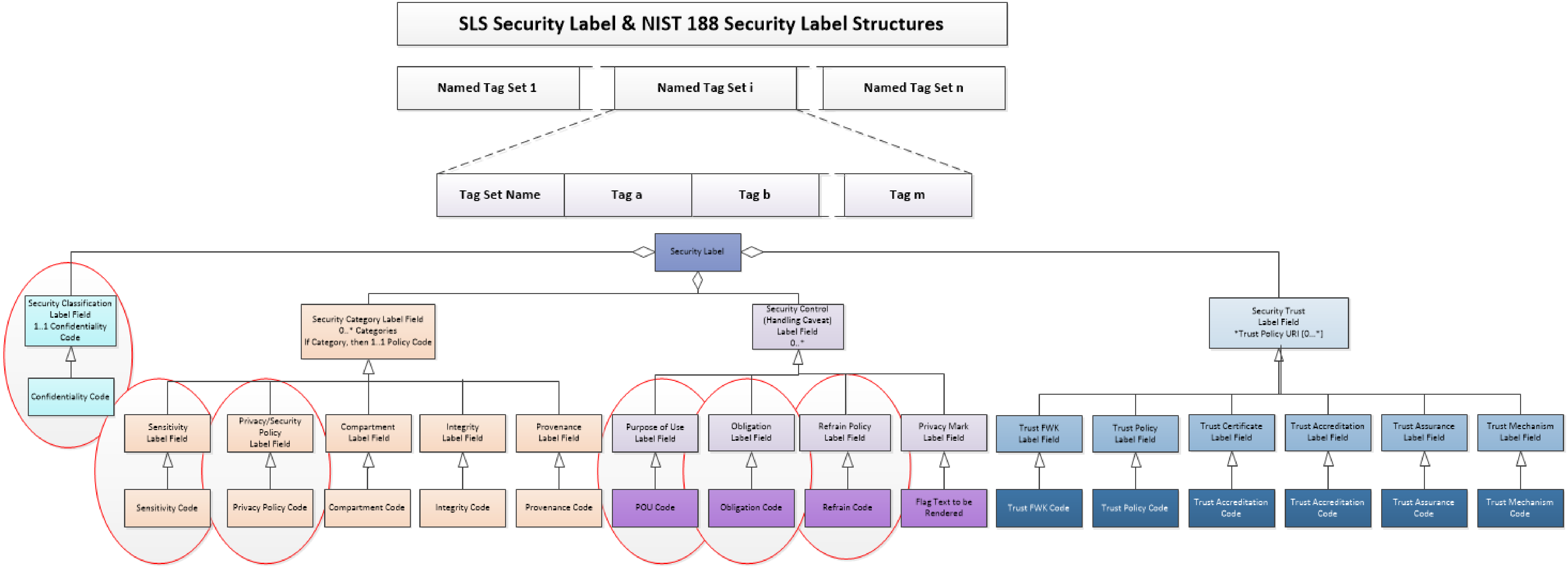
Sensitivity is the 0..* component of a Security Label that conveys the value, importance, and vulnerability of an IT resource perceived as undesirable to share.

Policy is the 0..1 component of a Security Label that conveys a mandate, obligation, requirement, rule, or expectation relating to its privacy.

Obligation is the 0..* component of a Security Label that conveys the mandated workflow action that an information custodian, receiver, or user must perform.

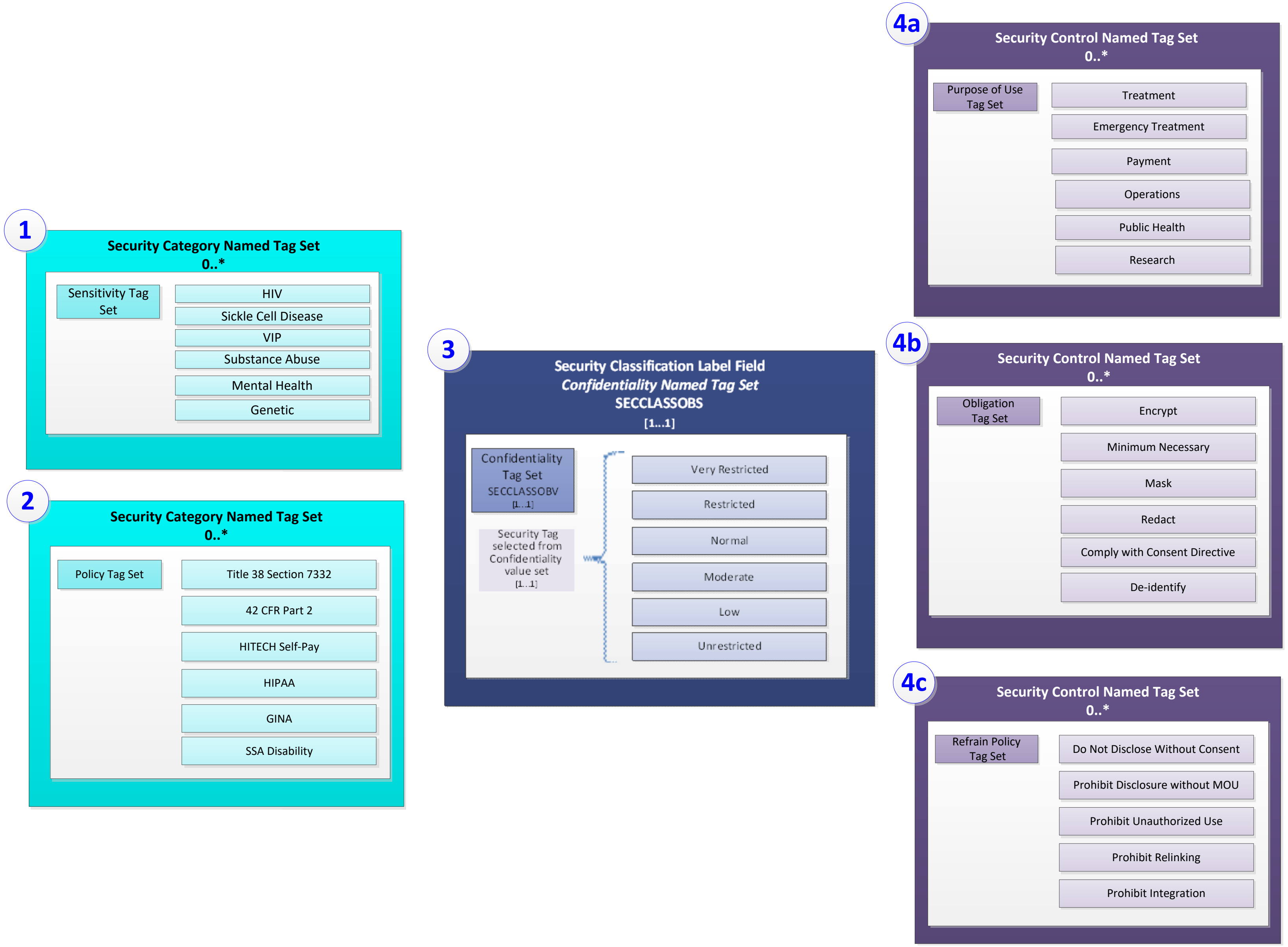
Refrain is the 0..* component of a Security Label that conveys actions which an information custodian, receiver, or user is not permitted to perform unless otherwise authorized or permitted under specified circumstances.

Only a Priority Subset of Tags are included in USCDI



Constructing Security Labels with Priority Tags

1. Community deems information sensitive based on risk that it could be used to stigmatize the information target.
2. If there is a governing policy, then determine:
3. Confidentiality level of protection afforded the information
4. Purpose of use restrictions on collection, access, use, or disclosure
5. Obligation policies mandating actions by Senders/Receivers
6. Refrain policies prohibiting actions by Senders/Receivers



1

Security Category Named Tag Set
0..*

Sensitivity Tag Set: HIV; Sickle Cell Disease; VIP; Substance Abuse; Mental Health; Genetic

2

Security Category Named Tag Set
0..*

Policy Tag Set: Title 38 Section 7332; 42 CFR Part 2; HITECH Self-Pay; HIPAA; GINA; SSA Disability

3

Security Classification Label Field
Confidentiality Named Tag Set
SECCLASSOBS
[1...1]

Confidentiality Tag Set
SECCLASSOBV
[1...1]

Security Tag selected from Confidentiality value set
[1...1]

Very Restricted; Restricted; Normal; Moderate; Low; Unrestricted

4a

Security Control Named Tag Set
0..*

Purpose of Use Tag Set: Treatment; Emergency Treatment; Payment; Operations; Public Health; Research

4b

Security Control Named Tag Set
0..*

Obligation Tag Set: Encrypt; Minimum Necessary; Mask; Redact; Comply with Consent Directive; De-identify

4c

Security Control Named Tag Set
0..*

Refrain Policy Tag Set: Do Not Disclose Without Consent; Prohibit Disclosure without MOU; Prohibit Unauthorized Use; Prohibit Relinking; Prohibit Integration

Security Label in USCDI – Use Case Descriptions

Needed to enable:

- Computably managed and enforced Privacy Consent Directives and Individual Right of Access requests for disclosures to third parties
- CEHRT implementers of the optional document and granular Data Segmentation certification criteria
- Granular privacy protection of minors', mothers', abuse victims, and seniors' health information as described in Protecting Privacy to Promote Interoperability use cases
- Consumer's control of shared health information as promoted by several Privacy Frameworks proposed by eHealth Exchange and Center for Democratic Technology; AMA; Carin Alliance; and others.

Security Label in USCDI – Use Case Descriptions

Further, Security Label adoption would enable computable data segmentation rather than requiring manual segmentation, where feasible, under the Information Blocking provisions.

HL7 Data Withholding Request to Prevent Harm is an example where Security Labels could document an Information Blocking exception and computably

- Specify that a Lab is not permitted to release results until the Ordering Provider has had an opportunity to discuss these with the patient based on concern of substantial harm – e.g., emotional distress about an adverse lab result
- Enable providers to withhold releasing information to parents/personal representatives based on concern of physical harm or patient request

HL7 has recently recommended that ONC move Confidentiality and Purpose of Use Tags from Level 1 to Level 2 for adoption in the 2022 USCDI for the protection of the increasing number of sensitive USCDI classes and elements also moving into the next version of USCDI.

HL7 also recommended that Sensitivity, Policy, Obligation, and Refrain Tags be moved to Level 1 as part of the minimum set needed to construct Security Labels for priority US interoperability use cases to enable Sharing with Protection.

Security Labeling Overview

This section provides a high level introduction to Security Labeling, which is not FHIR specific.

Confluence Background on Security Labels

FHIR Security Labels

Tutorial Webinar Recordings also available:

Security Labeling for PP2PI.pptx

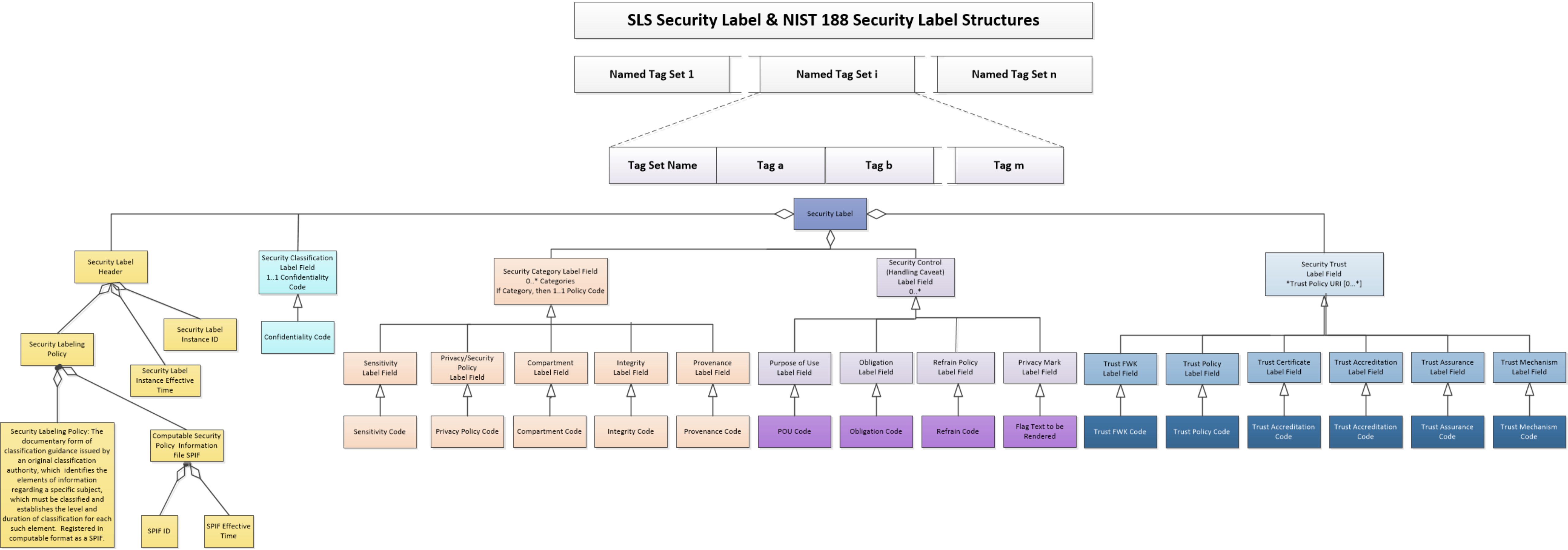
Security Labeling for PP2PI second.pptx

Share with Protections

“Share with Protections” is an information exchange paradigm that describes an environment of continuous end-to-end protection and trust for information shared by senders, thereafter received, retained and used by receivers, and backed by healthcare systems using automation. Core features include:

- Senders attach standards-based Security Labels to information indicating its relative sensitivity for sharing with trusted recipients and any handling instructions,
- Recipients honor, retain, and enforce senders’ labels by managing policy-driven access to information based on machine-computable sensitivity rules, “need to know,” and application of least privilege and segregation of duties within their own workforce, and
- Patient safety enabled through Emergency Access, utilizing Clinical Decision Support, and clinician break-glass priorities.
- Share with Protections recommends standard Role- or Attribute-based access control (RBAC/ABAC) services for information classification and user clearances as a best approach to protecting an organization’s healthcare mission, patient privacy and to optimize clinician support. See the Share with Protections White Paper Project.

Security Label Named Tag Sets – Value Set Types



SLS Security Label & NIST 188 Security Label Structures

Named Tag Set 1

Named Tag Set i

Named Tag Set n

Tag Set Name

Tag a

Tag b

Tag m

Security Label

Security Label Header

Security Labeling Policy

Security Label Instance ID

Security Label Instance Effective Time

Security Labeling Policy: The documentary form of classification guidance issued by an original classification authority, which identifies the elements of information regarding a specific subject, which must be classified and establishes the level and duration of classification for each such element. Registered in computable format as a SPIF.

Computable Security Policy Information File SPIF

SPIF ID

SPIF Effective Time

Security Classification Label Field 1..1 Confidentiality Code

Confidentiality Code

Security Category Label Field 0..* Categories If Category, then 1..1 Policy Code

Sensitivity Label Field

Sensitivity Code

Privacy/Security Policy Label Field

Privacy Policy Code

Compartment Label Field

Compartment Code

Integrity Label Field

Integrity Code

Provenance Label Field

Provenance Code

Security Control (Handling Caveat) Label Field 0..*

Purpose of Use Label Field

POU Code

Obligation Label Field

Obligation Code

Refrain Policy Label Field

Refrain Code

Privacy Mark Label Field

Flag Text to be Rendered

Security Trust Label Field *Trust Policy URI [0...*]

Trust FWK Label Field

Trust FWK Code

Trust Policy Label Field

Trust Policy Code

Trust Certificate Label Field

Trust Accreditation Code

Trust Accreditation Label Field

Trust Accreditation Code

Trust Assurance Label Field

Trust Assurance Code

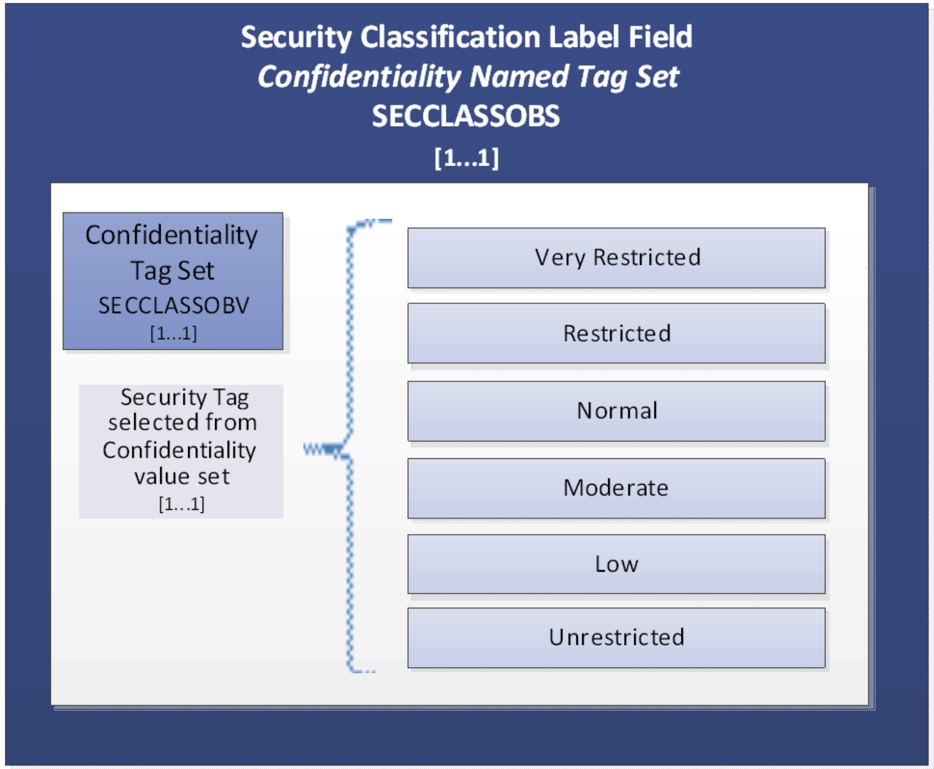
Trust Mechanism Label Field

Trust Mechanism Code

https://confluence.hl7.org/display/SEC/Security+Labeling+System+and+Technical+Requirements?preview=/61506175/113672210/Security%20Label%20Structure%20DS4P%20MJ.png

Security Label Named Tag Sets

Security Classification Type of security metadata observation made about the classification of an IT resource (data, information object, service, or system capability), which may be used to make access control decisions. Security classification is defined by ISO/IEC 2382-8:1998(E/F)/ T-REC-X.812-1995 as: *“The determination of which specific degree of protection against access the data or information requires, together with a designation of that degree of protection.”*



Security Classification Label Field
Confidentiality Named Tag Set
SECCLASSOBS
[1...1]

Confidentiality Tag Set
SECCLASSOBV
[1...1]

Security Tag selected from Confidentiality value set
[1...1]

- Very Restricted
- Restricted
- Normal
- Moderate
- Low
- Unrestricted

Security label metadata classifying an IT resource (clinical fact, data, information object, service, or system capability) according to its level of sensitivity

Based on an analysis of applicable privacy policies and the risk of financial, reputational, or other harm to an individual or entity that could result if made available or disclosed to unauthorized individuals, entities, or processes.

Mandatory, single most important Security Tag.

Minimum conveyance of the Access Control protections.

Security Category Named Tag Sets

Type of security metadata observation made about the category of an IT resource (data, information object, service, or system capability), which may be used to make access control decisions. Security category metadata is defined by ISO/IEC 2382-8:1998(E/F)/ T-REC-X.812-1995 as: *"A nonhierarchical grouping of sensitive information used to control access to data more finely than with hierarchical security classification alone."*

Tag Set	Card.	Description	Example Tags
Policy	0..1	Security label metadata that segments an IT resource by conveying a mandate, obligation, requirement, rule, or expectation relating to its privacy.	HIPAA, Part 2
Sensitivity	0..*	Security label metadata that segments an IT resource by categorizing the value, importance, and vulnerability of an IT resource perceived as undesirable to share.	STD, HIV, SUD
Compartment	0..*	Security label metadata that segments an IT resource by indicating that access and use is restricted to members of a defined community or project.	Care Team, Research Project
Integrity	0..*	Security label metadata that segments an IT resource by conveying the completeness, veracity, reliability, trustworthiness, and provenance of an IT resource.	Anonymized, Digitally signed
Provenance	0..*	Security label metadata that segments an IT resource by conveying the provenance of the IT resource's asserted or reported source.	Patient reported, Clinician asserted
Trust	0..*	Security label metadata that segments an IT resource by conveying the basis for trusting the source.	Trust Accreditation, Trust Agreement

Security Control Named Tag Sets

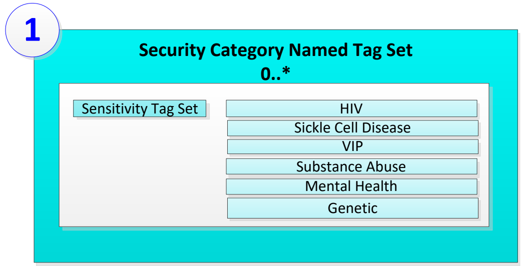
Type of security metadata observation made about the control of an IT resource (data, information object, service, or system capability), which may be used to make access control decisions. Security control metadata conveys instructions for secure distribution, transmission, storage or use.

Tag Set	Card.	Description	Example Tags
Purpose of Use	0..*	Security label metadata that segments an IT resource by conveying the reason for performing one or more operations on information, which may be permitted by source system's security policy in accordance with one or more privacy policies and consent directives.	Treatment, Payment, Operation, Research
Obligation	0..*	Security label metadata that segments an IT resource by conveying the mandated workflow action that an information custodian, receiver, or user must perform.	Encrypt, mask, comply wih policy
Refrain	0..*	Security label metadata that segments an IT resource by conveying actions which an information custodian, receiver, or user is not permitted to perform unless otherwise authorized or permitted under specified circumstances.	Do not disclose without consent, no reuse
CUI Privacy Mark	0..*	Security label metadata that segments an IT resource by conveying a displayed mark, required to be rendered to indicate that the electronic or hardcopy information is protected at the level of the subset of CUI for which the authorizing law, regulation, or Government-wide policy does not set out specific handling or dissemination controls.	CUI, SP-CUI
Security Label Mark	0..*	Security label metadata that segments an IT resource by conveying a displayed mark rendered as specified.	Draft, Confidential
Security Authorization Policy	0..*	Security label metadata that segments an IT resource by conveying specific permissions used for access control.	Authorization policy, Delegation policy

Constructing Security Labels

1. Community deems information sensitive based on risk that it could be used to stigmatize the information target.
2. If there is a governing policy, then determine:
3. Confidentiality level of protection afforded the information
4. Purpose of use restrictions on collection, access, use, or disclosure
5. Obligation policies mandating actions by Senders/Receivers
6. Refrain policies prohibiting actions by Senders/Receivers

1

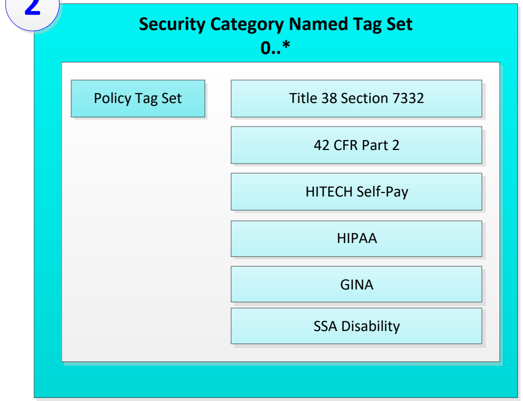


Security Category Named Tag Set
0..*

Sensitivity Tag Set

- HIV
- Sickle Cell Disease
- VIP
- Substance Abuse
- Mental Health
- Genetic

2

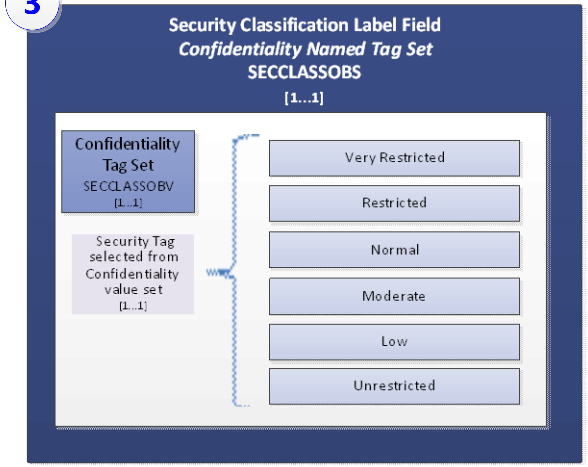


Security Category Named Tag Set
0..*

Policy Tag Set

- Title 38 Section 7332
- 42 CFR Part 2
- HITECH Self-Pay
- HIPAA
- GINA
- SSA Disability

3



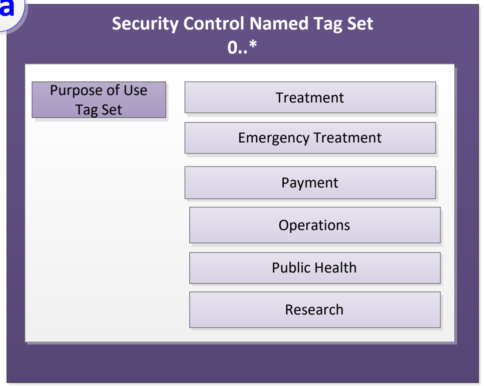
Security Classification Label Field
Confidentiality Named Tag Set
SECCLASSOBS
[1...1]

Confidentiality Tag Set
SECCLASSOBV
[1...1]

Security Tag selected from Confidentiality value set
[1...1]

- Very Restricted
- Restricted
- Normal
- Moderate
- Low
- Unrestricted

4a

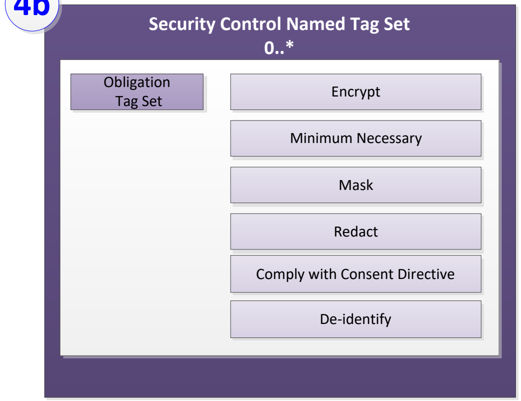


Security Control Named Tag Set
0..*

Purpose of Use Tag Set

- Treatment
- Emergency Treatment
- Payment
- Operations
- Public Health
- Research

4b

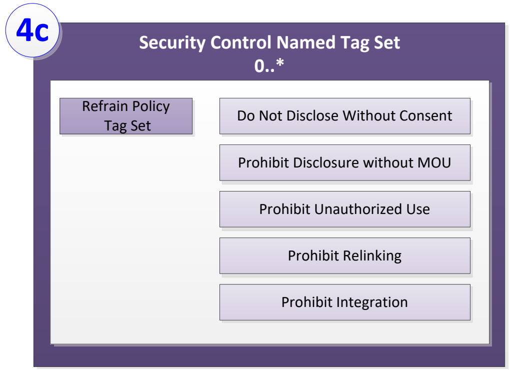


Security Control Named Tag Set
0..*

Obligation Tag Set

- Encrypt
- Minimum Necessary
- Mask
- Redact
- Comply with Consent Directive
- De-identify

4c

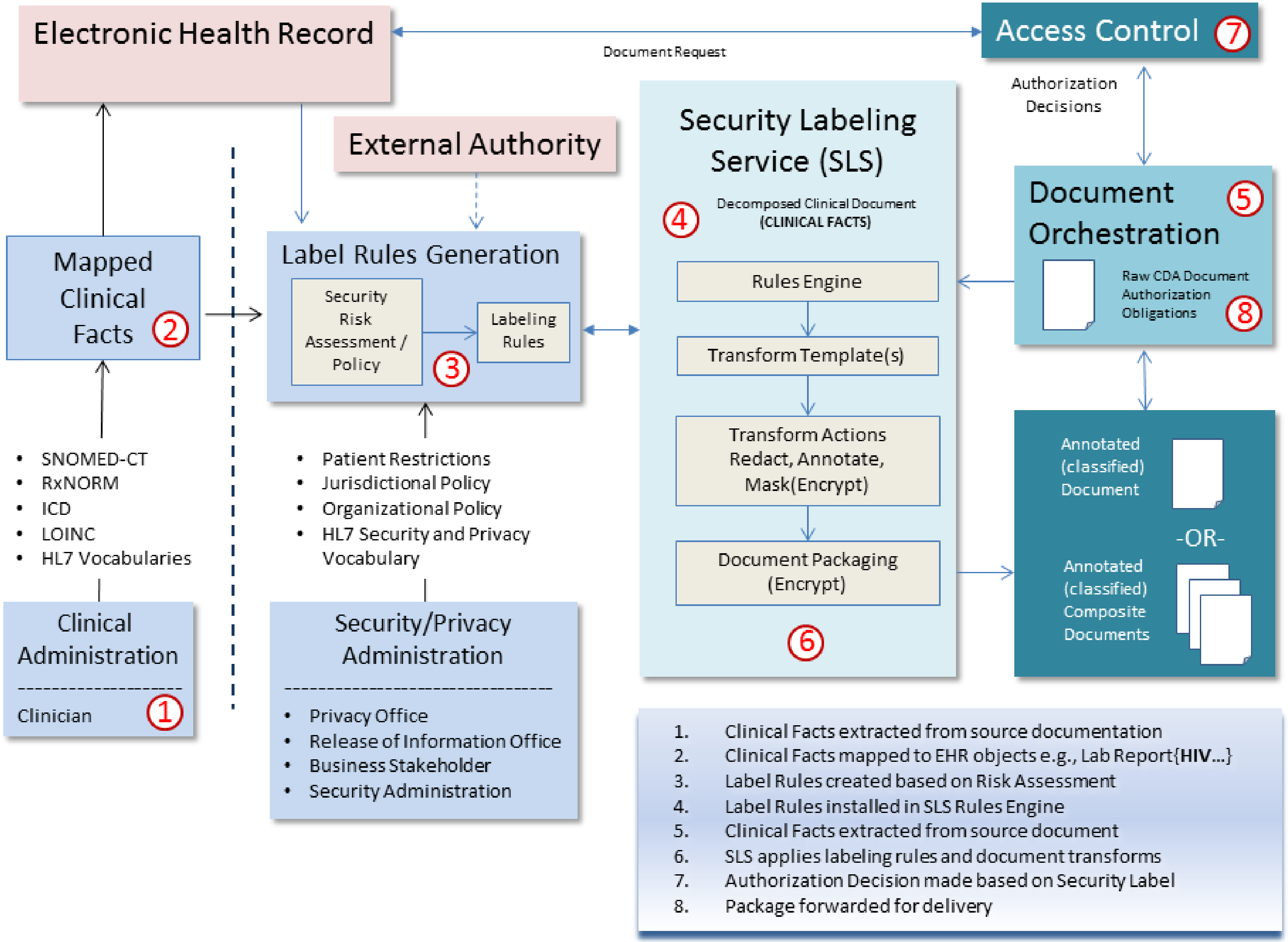


Security Control Named Tag Set
0..*

Refrain Policy Tag Set

- Do Not Disclose Without Consent
- Prohibit Disclosure without MOU
- Prohibit Unauthorized Use
- Prohibit Relinking
- Prohibit Integration

Security Labeling Workflow



Electronic Health Record

Document Request

Access Control 7

Authorization Decisions

External Authority

Mapped Clinical Facts 2

Label Rules Generation

Security Risk Assessment / Policy

Labeling Rules

3

Security Labeling Service (SLS)

4 Decomposed Clinical Document (CLINICAL FACTS)

Rules Engine

Transform Template(s)

Transform Actions Redact, Annotate, Mask(Encrypt)

Document Packaging (Encrypt)

6

Document Orchestration 5

Raw CDA Document
Authorization
Obligations 8

Annotated (classified) Document

-OR-

Annotated (classified) Composite Documents

- SNOMED-CT
- RxNORM
- ICD
- LOINC
- HL7 Vocabularies

Clinical Administration

Clinician 1

- Patient Restrictions
- Jurisdictional Policy
- Organizational Policy
- HL7 Security and Privacy Vocabulary

Security/Privacy Administration

- Privacy Office
- Release of Information Office
- Business Stakeholder
- Security Administration

1. Clinical Facts extracted from source documentation
2. Clinical Facts mapped to EHR objects e.g., Lab Report{**HIV…**}
3. Label Rules created based on Risk Assessment
4. Label Rules installed in SLS Rules Engine
5. Clinical Facts extracted from source document
6. SLS applies labeling rules and document transforms
7. Authorization Decision made based on Security Label
8. Package forwarded for delivery

Informatics, Policy, and Technical Capabilities:

- Clinical Informaticists establish sensitive information value sets to filter structured data and NLP of unstructured data
- Determine applicable privacy/security policies including patient preferences
- Security Labeling Service filters requested information to determine any sensitivity and applicable policy based on contextual inputs
- Privacy Protective Services transform, redact, or mask based on assigned labels
- Access Control decisions made based on the clearance of the requester/recipient

Key Terms - Security Label

As a Verb: "means used to associate security attributes" as in "security labeling"

- The means used to associate a set of security attributes with a specific information object as part of the data structure for that object [ISO 10181-3/ITU X.812].

As a noun synonymous with "security metadata" and "security tag"

- Access control information associated with the attribute values being accessed [ISO/IEC 9594-2:2008/ITU X.501].

- The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource. NOTE - The marking and/or binding may be explicit or implicit [ISO 7498-2].

As both the classification given to IT resources and the classification level in an initiator's clearance.

- A security label, sometimes referred to as a confidentiality label, is a structured representation of the sensitivity of a piece of information. A security label is used in conjunction with a clearance, a structured representation of what information sensitivities a person (or other entity) is authorized to access and a security policy to control access to each piece of information [XMPP Core].

As a "marking bound to a resource" to refer to both computable security labels and the human-readable rendering of security label fields, better known as "privacy markings"

Key Terms

- **Security Tag** Information unit containing a representation of certain security-related information (e.g., a restrictive attribute bit map) [NIST FIPS PUB 188].
- **Security (Labeling) Policy** The definition of which classification and category values are used and how security labels are checked against clearances.
- **Security Label Rule** A computational algorithm used for assigning a security label to an IT resource such as a clinical fact.
- **Security Policy Information File (SPIF)** A construct that conveys domain-specific security policy information [ISO/IEC 15816].
- **Tag Set Name** Numeric identifier associated with a set of security tags [NIST FIPS PUB 188]. In HL7 terms, a Tag Set Name = Tag Value Set Identifier

Security Label in USCDI – Use Case Descriptions

Further, Security Label adoption would enable computable data segmentation rather than requiring manual segmentation, where feasible, under the Information Blocking provisions.

HL7 Data Withholding Request to Prevent Harm is an example where Security Labels could document an Information Blocking exception and computably

- Specify that a Lab is not permitted to release results until the Ordering Provider has had an opportunity to discuss these with the patient based on concern of substantial harm – e.g., emotional distress about an adverse lab result
- Enable providers to withhold releasing information to parents/personal representatives based on concern of physical harm or patient request

HL7 has recently recommended that ONC move Confidentiality and Purpose of Use Tags from Level 1 to Level 2 for adoption in the 2022 USCDI for the protection of the increasing number of sensitive USCDI classes and elements also moving into the next version of USCDI.

HL7 also recommended that Sensitivity, Policy, Obligation, and Refrain Tags be moved to Level 1 as part of the minimum set needed to construct Security Labels for priority US interoperability use cases to enable Sharing with Protection.

USCDI Security Label Details

The following slides include excerpts from the USCDI listings for Security Labels.

Slide Titles are links to the USCDI pages where these are lists.

Each tag code links to its HL7 Terminology value set.

Confidentiality Tag - USCDI Level 1

Confidentiality codes are required in all CDA profiles, including C-CDA, at the Document header class, in the HL7 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1, in the HL7 Version 2.9 BHS, FHS, MSH, and ARV Segments, and in the FHIR Data Segmentation for Privacy IG.

These standards require that the appropriate Confidentiality code required by the governing policy be included. E.g., if the content is governed by HIPAA, the Confidentiality code must be “N” for the normal level of protection for healthcare information in the US realm. If the content is governed as additionally protected information, the Confidentiality code must be “R” for a restricted level of access.

If the content is released outside of HIPAA or laws that more stringently protect confidentiality, such as when an individual exercises HIPAA Right of Access, then the Confidentiality code must be “M” for moderate protections under laws that are less protective than HIPAA, such as FTC Consumer Protection Laws.

The Confidentiality tag is a mandatory component of a Security Label, the meaning of which is understood in the context of the set of relevant tags representing a policy.

Confidentiality tags are Confidentiality codes in the HL7 Confidentiality Code System.

Confidentiality codes (links to value set) convey the type of privacy metadata classifying an IT resource (data, information object, service, or system capability) according to its level of sensitivity, which is based on an analysis of applicable privacy policies and the risk of financial, reputational, or other harm to an individual or entity that could result if made available or disclosed to unauthorized individuals, entities, or processes.

Usage Note: Confidentiality codes may be used in security labels and privacy markings to classify IT resources based on sensitivity to indicate the obligation of a custodian or receiver to ensure that the protected resource is not made available or disclosed to individuals, entities, or processes (security principals) unless authorized per applicable policies. Confidentiality codes may also be used in the clearances of initiators requesting access to protected resources.

Purpose of Use Tag - USCDI Level 1

A Purpose of Use tag is the 0..* component of a Security Label that conforms to follows the HL7 Healthcare Privacy and Security Classification System (HCS), Release 1 syntax to indicate the circumstances under which an authorized recipient is permitted to perform an activity such as create, collect, access, use, or disclose.

Purpose of Use tags are Purpose of Use codes in the HL7 Act Reason Code System.

Purpose of Use codes (links to value set) convey the reason for performing one or more operations on information, which may be permitted by source system's security policy in accordance with one or more privacy policies and consent directives.

Usage Notes: The rationale or purpose for an act relating to the management of personal health information, such as collecting personal health information for research or public health purposes.

Sensitivity Tag - USCDI Comment

A Sensitivity tag is the 0..* component of a Security Label that conforms to the HL7 Healthcare Privacy and Security Classification System (HCS), Release 1 syntax to represent the type of information deemed by policy to require a specified level of Confidentiality protection.

Sensitivity tags are Information Sensitivity codes in the HL7 Act Code System.

Information Sensitivity codes (links to value set) conveys a mandate, obligation, requirement, rule, or expectation characterizing the value or importance of a resource and may include its vulnerability. (Based on ISO7498-2:1989. Note: The vulnerability of personally identifiable sensitive information may be based on concerns that the unauthorized disclosure may result in social stigmatization or discrimination.)

A sensitivity policy is adopted by an enterprise or group of enterprises (a 'policy domain') through a formal data use agreement that stipulates the value, importance, and vulnerability of information.

A sensitivity code representing a sensitivity policy may be associated with criteria such as categories of information or sets of information identifiers (e.g., a value set of clinical codes or branch in a code system hierarchy). These criteria may in turn be used for the Policy Decision Point in a Security Engine.

Policy Tag - USCDI Comment

A Policy tag is the 0..1 component of a Security Label that conforms to follows the HL7 Healthcare Privacy and Security Classification System (HCS), Release 1 syntax to represent the policy governing of the information assigned a Security Label.

The policy represented by this code is the authoritative source of the type of information deemed sensitive and the level of confidentiality protection to be provided.

Policies may pertain to privacy, security, research, trust, etc., and may be issued by a jurisdiction, an organization, or an individual, e.g., by a consent directive.

In addition, the policy may limit the permissible purposes of use, and the obligations and prohibited actions which may be taken by senders and receivers, which are conveyed using other types of tags in the Security Label representing a specific policy.

Policy Tags are Policy codes in the HL7 Act Code System.

Policy codes (links to value set) convey a mandate, regulation, obligation, principle, requirement, rule, or expectation of how an entity is to conduct itself or execute an activity, which may be dictated and enforced by an authority of competent jurisdiction.

Obligation Tag – USCDI Comment

An Obligation tag is the 0..* component of a Security Label that conforms to follows the HL7 Healthcare Privacy and Security Classification System (HCS), Release 1 syntax to convey the mandated action that an information custodian, receiver, or user must perform.

Obligation Tags are Obligation Policy codes in the HL7 Act Code System.

Obligation Policy codes (links to value set) convey the mandated workflow action that an information custodian, receiver, or user must perform.

Usage Notes: Per ISO 22600-2, ObligationPolicy instances 'are event-triggered and define actions to be performed by manager agent'.

Per HL7 Composite Security and Privacy Domain Analysis Model: This value set refers to the action required to receive the permission specified in the privacy rule. Per OASIS XACML, an obligation is an operation specified in a policy or policy that is performed in conjunction with the enforcement of an access control decision.

Refrain Tag – USCDI Comment

A Refrain tag is the 0..* component of a Security Label that conforms to follows the HL7 Healthcare Privacy and Security Classification System (HCS), Release 1 syntax to convey a prohibited action that an information custodian, receiver, or user must not perform.

Refrain tags are Refrain Policy codes in the HL7 Act Code System.

Refrain Policy codes (links to value set) convey prohibited actions which an information custodian, receiver, or user is not permitted to perform unless otherwise authorized or permitted under specified circumstances.

Usage Notes: ISO 22600-2 species that a Refrain Policy "defines actions the subjects must refrain from performing". Per HL7 Composite Security and Privacy Domain Analysis Model: May be used to indicate that a specific action is prohibited based on specific access control attributes e.g., purpose of use, information type, user role, etc.

References

- FHIR Data Segmentation for Privacy 0.2.0 - 2021May Ballot
- HL7 Confluence Security Labels – for detailed discussion
- HIMSS Interoperability Showcase 202002 - Consumer Centered Care Planning Use Case Video
- Privacy on FHIR HIMSS 2015 Security Labeling Demo
- Health Privacy Summit 2013 DS4P VA-SAMHSA Pilot

Break

See you in 5!

HEART Overview and SDOH

Nancy Lush

Patient Centric Solutions, Inc.

The Office of the National Coordinator for
Health Information Technology

DEPARTMENT OF HEALTH & HUMAN SERVICES • USA

Gaps in Care

- Needs to see a specialist outside of her healthcare system
- Share health data with a spouse or adult child
- Share health data with a research organization
- A new provider does not have access to a patient’s record
- Ability to share relevant device data
- Needs to keep some aspects of their data private
- Patients travel or relocate seasonally
- Transitions of Care

Why HEART?

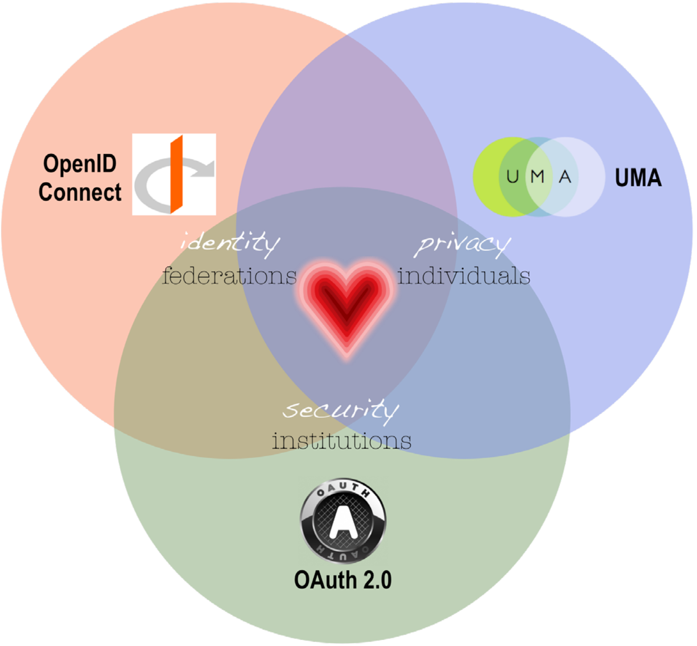
- Created to address these challenges and gaps
- Enables the patient to safely share their health records with users of their choice, in an interoperable way that respects and honors patient security and privacy
- Enables patient directed sharing of their clinical data

What is HEART?

HEART (HEAlth Relationship Trust) is a set of profiles that enable patients to control how, when, and with whom their clinical data is shared.

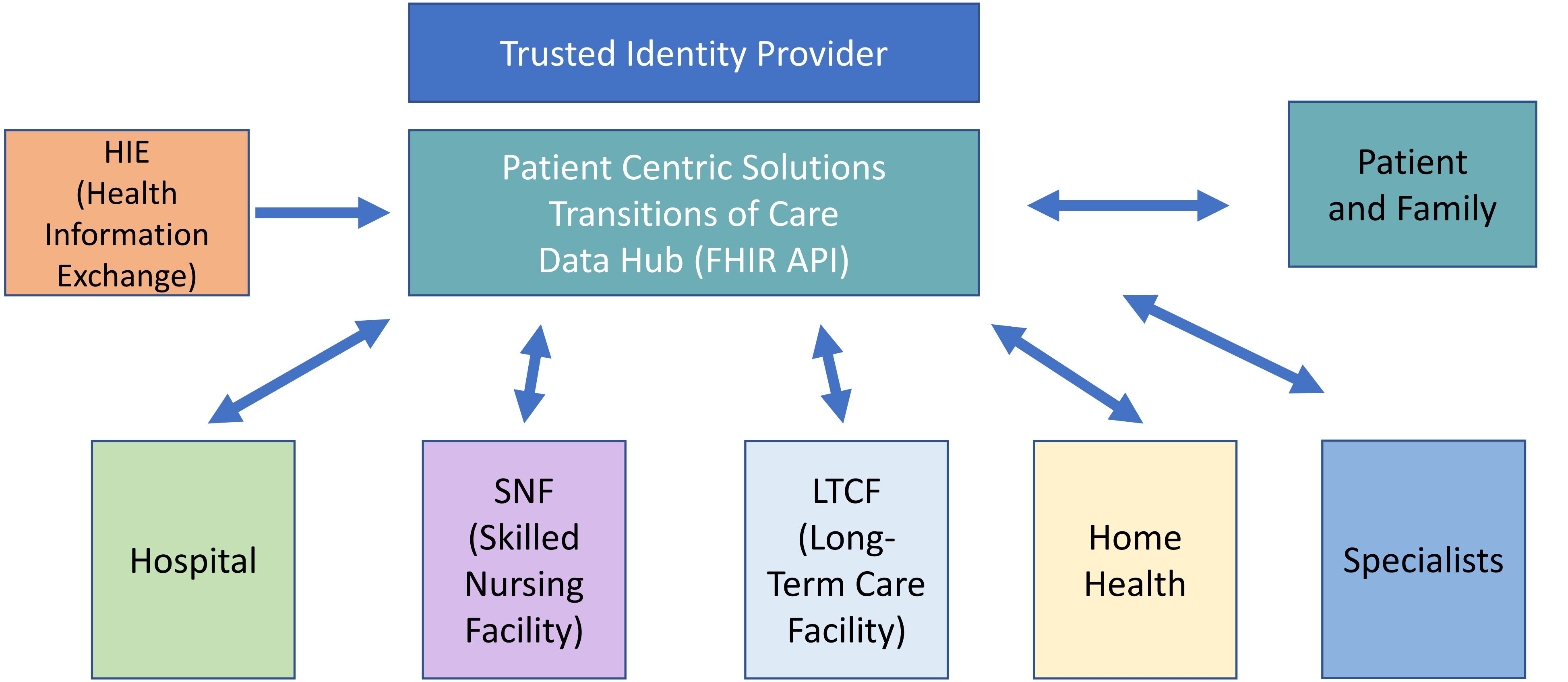
What is HEART?

- Leverages existing open standards
  - FHIR / SMART on FHIR
  - OAuth 2
  - OpenID Connect
  - User Managed Access
- Best practice security standards
- Adds additional security features
- Gives patients control over how their data is shared
- Defines interoperable process for patient directed clinical data sharing



HEART Benefits

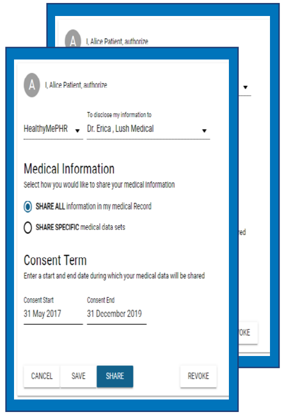
1. HEART enables patient directed **sharing** across a wide ecosystem


Trusted Identity Provider
HIE (Health Information Exchange)
Patient Centric Solutions
Transitions of Care
Data Hub (FHIR API)
Patient and Family
Hospital
SNF (Skilled Nursing Facility)
LTCF (Long-Term Care Facility)
Home Health
Specialists

HEART Benefits

2. The patient controls who has access to their data

- Gives patients control over how their data is shared
- Electronic consents define patient’s sharing wishes
- Authorization is based on patient-specified policy
- Enables multi-party sharing
- Authorization is provided asynchronously
- The patient makes the decision on who has access to their data



I, Alice Patient, authorize

HealthyMePHR

To disclose my information to

Dr. Erica , Lush Medical

Medical Information

Select how you would like to share your medical information

● **SHARE ALL** information in my medical Record

○ **SHARE SPECIFIC** medical data sets

Consent Term

Enter a start and end date during which your medical data will be shared

Consent Start: 31 May 2017

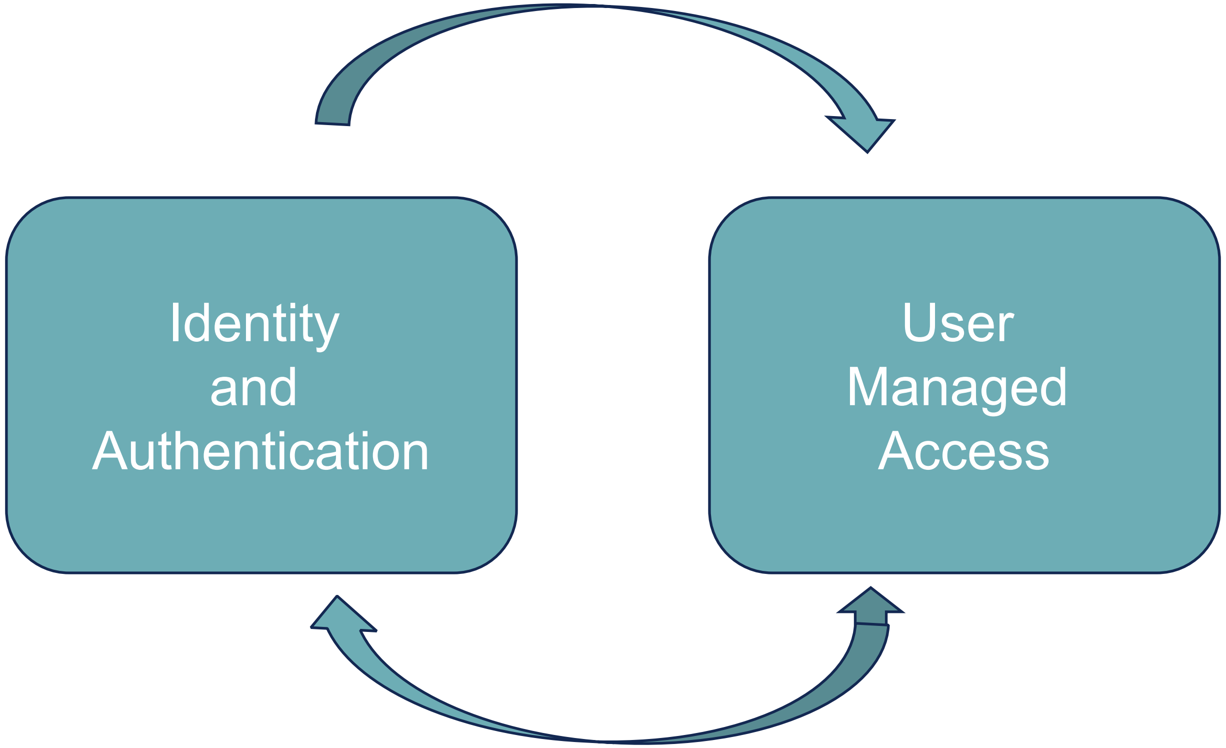
Consent End: 31 December 2019

HEART Benefits

3. HEART works in conjunction with Best Practice Security Standards

- We want to know that our patient Alice is really Alice
- We want to know that the user requesting information is who they say they are
- Ideally, users are identified through identity assurance. They only need to be identity proofed once, for that to apply to a high level of authentication.
- The user can be authenticated through high level trusted authentication systems

Two Enabling Technologies



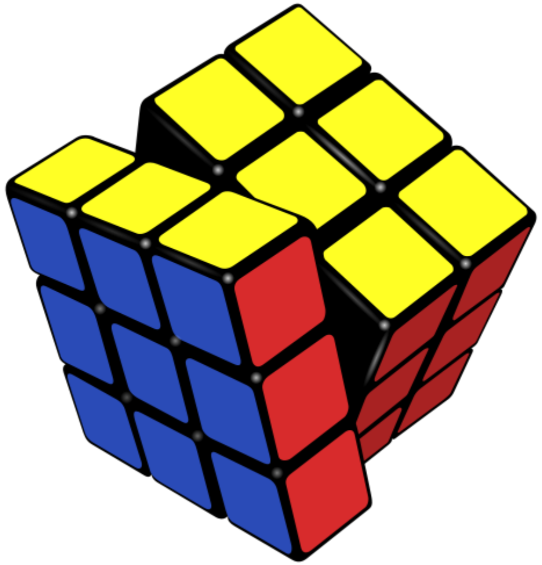
Identity and Authentication

User Managed Access

HEART Benefits

4. HEART provides more granular management over protected resources

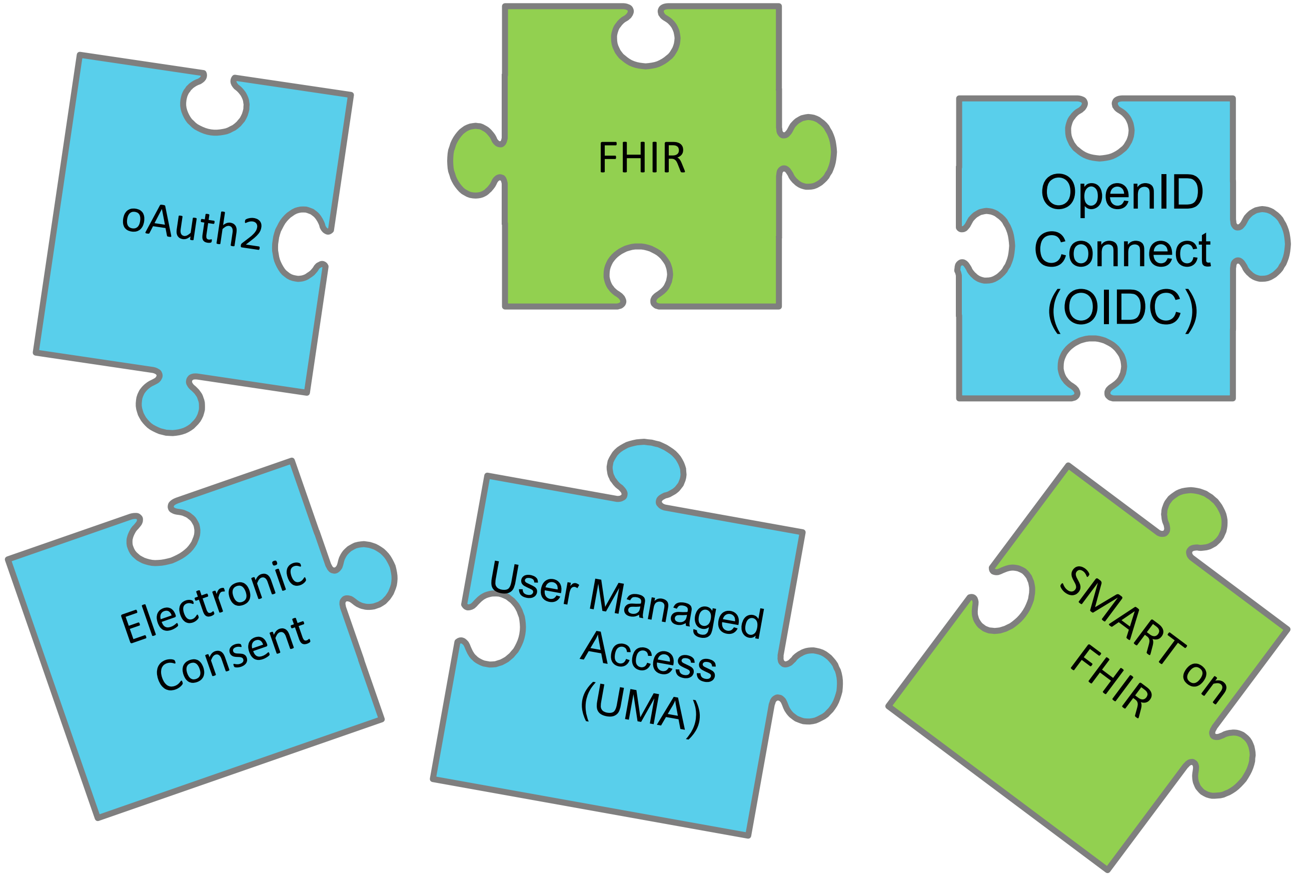
- Control over Who/What/How at a fine grain
- Which Resource?
- What Scopes?
- What Sensitive Data?



HEART Benefits

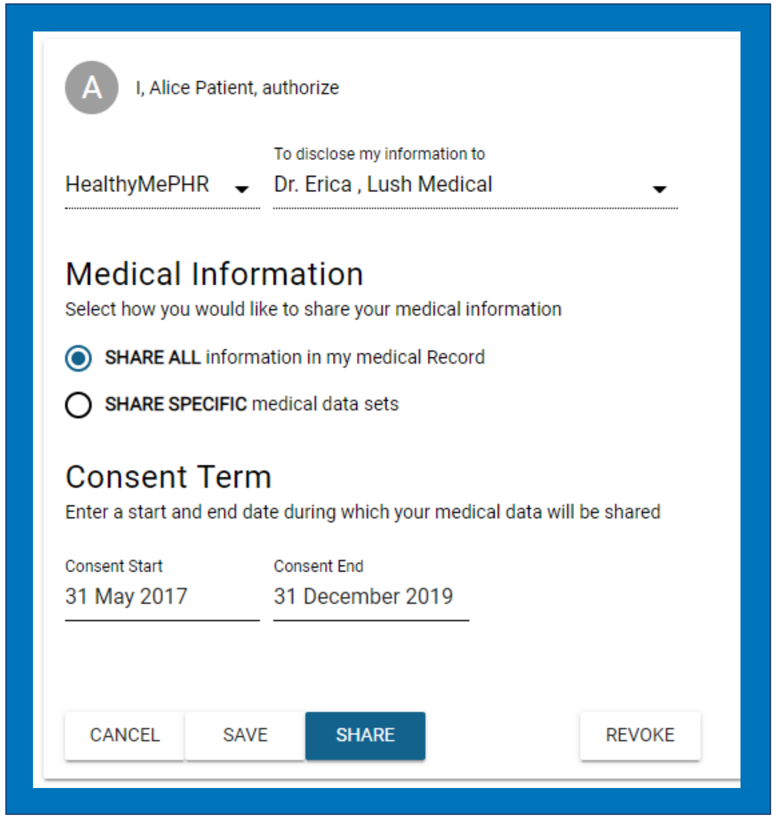
5. Leverages existing open standards

- FHIR / SMART on FHIR
- OAuth 2
- OpenID Connect
- User Managed Access



HEART Benefits

6. HEART Patient and Provider clients are EASY to use



A I, Alice Patient, authorize

HealthyMePHR ▾

To disclose my information to
Dr. Erica , Lush Medical ▾

Medical Information

Select how you would like to share your medical information

● **SHARE ALL** information in my medical Record

○ **SHARE SPECIFIC** medical data sets

Consent Term

Enter a start and end date during which your medical data will be shared

Consent Start
31 May 2017

Consent End
31 December 2019

- Patient Alice creates a policy to share with Dr. Erica, she selects her sharing preferences, and presses SHARE

SHARE

- Patient sharing is easy!

HEART Benefits

7. Supports Data Segmentation for Privacy

- HEART included profiles for Confidentiality and Sensitivity data
- Work done in conjunction with SAMHSA, Consent 2 Share and data tagging projects with the intent to support data segmentation for privacy.
- HEART allows data to be exchanged dynamically while honoring patient privacy

HEART Benefits

1. HEART enables patient directed **sharing** across a wide ecosystem
2. The patient controls who has access to their data
3. HEART works in conjunction with Best Practice Security Standards
4. HEART provides more granular management over protected resources
5. Leverages existing open standards
6. HEART Patient and Provider clients are intended to be EASY to use
7. Supports Data Segmentation for Privacy

HEART Implementations

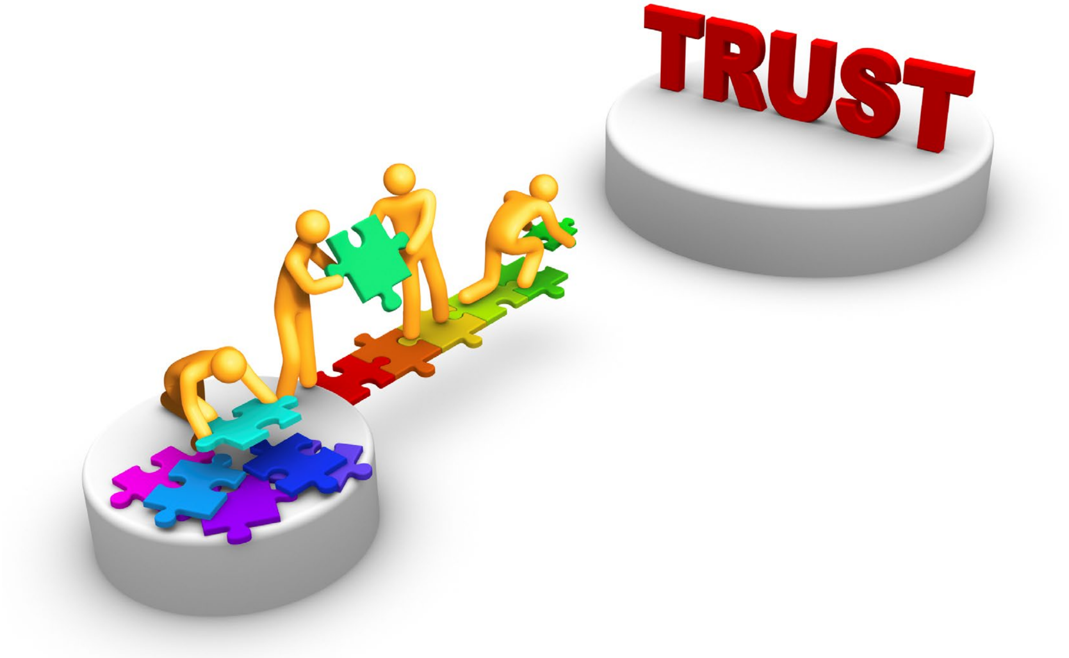
- EMR Direct/HealthToGo
- HIE of One/Trustee
- HealthyMePHR
- Patient*Share*

UMA2 Workgroup

- Kantara Initiative
- Continues to deep dive into applicable topics
- UMA Business-Legal-Technical
  - Use cases
  - Framework
  - Business Model Graphics
- Delegation
  - Not all patients can manage their own policy
  - Older or incapable patient
  - Child
  - Processes to transfer administration rights

HEART as it applies to Data Privacy

- Ability to define sharing policies at a granular level
  - Granularity can be defined
  - The technology can support many use cases
- In healthcare
  - Which resource?
  - What scopes?
  - What sensitive data?
- Security profiles
  - Specifically profiled by HEART as requested by SAMHSA
  - Sensitivity and Confidentiality scopes



Security Scopes

- Confidentiality
  - conf/N - Normal confidentiality
  - conf/R - Restricted confidentiality
  - conf/V - Very Restricted confidentiality
- Sensitivity Examples
  - sens/ETH - Substance abuse
  - sens/PSY - Psychiatry
  - sens/HIV - HIV/AIDS
  - sens/SOC - Social services
  - sens/SDV - Sexual assault, abuse, or domestic violence
  - sens/SEX - Sexuality and reproductive health

Existing Technologies in support of Privacy Interop

- Electronic Consents
  - Consent to Share (C2S), SAMHSA
  - Patient*Share,* Patient Centric Solutions
  - Digital Wallet, Identos
  - Others
- Value Sets - Mapped to sensitivity levels
- FHIR tagging/redaction engines
- HEART/UMA to manage secure exchange
- FHIR APIs
- Trusted Identity Servers and related standards

Current Blocks

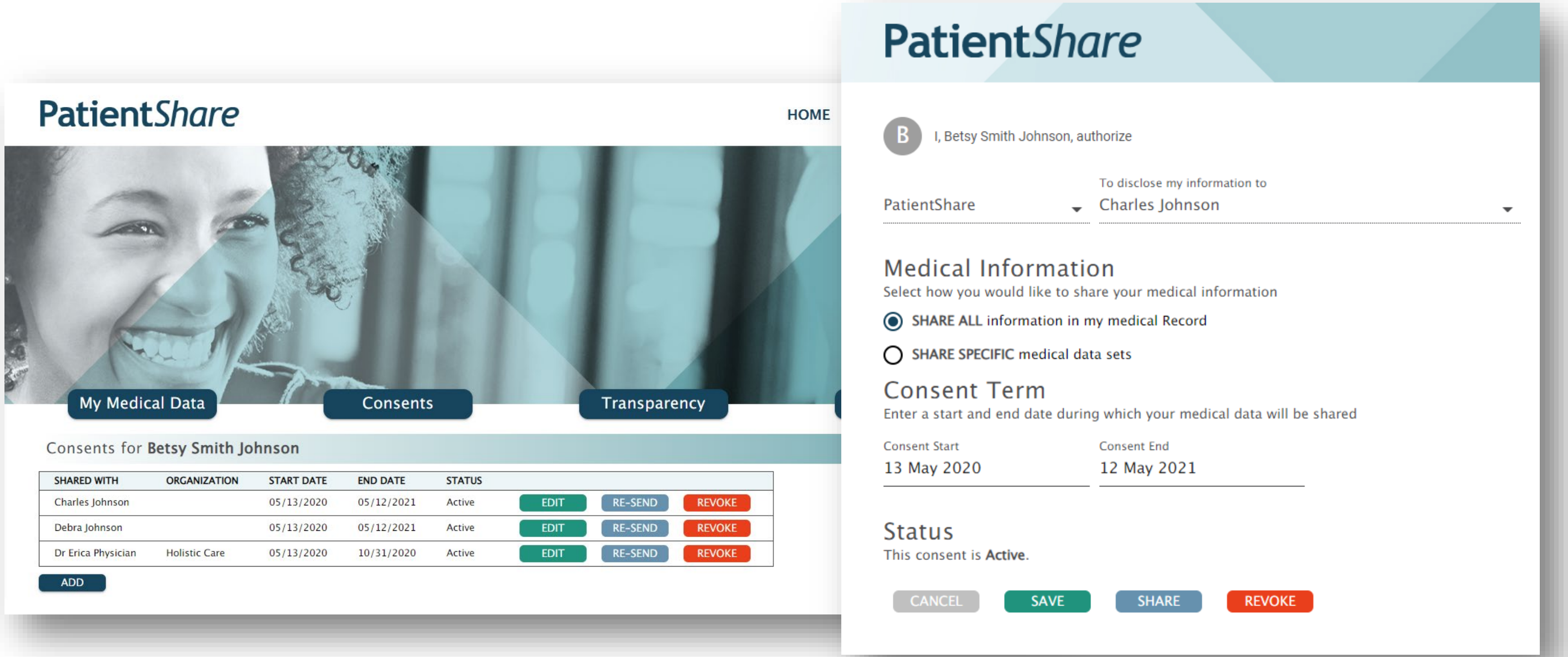
- Maintenance of Value Sets
- Data Segmentation encoding
  - Most data coming from FHIR APIs are not encoded.
  - AI proposals to encode
  - For our recent projects, the IG data IS encoded
    - PACIO – Post Acute Care Interoperability
    - eLTSS – Electronic Long Term Services & Support
    - SDOH – Social Determinants of Health
- Policies – Conflicts/Resolutions
- PP2PI WG just getting started
  - Protecting Privacy to Promote Interoperability

Patient Policies

- Patient-mediated exchange supports patient policies
- Premise:
  - Patient has right to their own data
  - Patient has right to share data as they wish
- Patient defines
  - Who has access to their data
  - What parts of their data they have access to
  - For how long
  - Can be revoked
- Delegation

Patient*Share* Consent

The patient or their delegate decides who has access to data.



Consents for **Betsy Smith Johnson**

SHARED WITH	ORGANIZATION	START DATE	END DATE	STATUS			
Charles Johnson		05/13/2020	05/12/2021	Active	EDIT	RE-SEND	REVOKE
Debra Johnson		05/13/2020	05/12/2021	Active	EDIT	RE-SEND	REVOKE
Dr Erica Physician	Holistic Care	05/13/2020	10/31/2020	Active	EDIT	RE-SEND	REVOKE

I, Betsy Smith Johnson, authorize

PatientShare

To disclose my information to: Charles Johnson

Medical Information

Select how you would like to share your medical information

● **SHARE ALL** information in my medical Record

○ **SHARE SPECIFIC** medical data sets

Consent Term

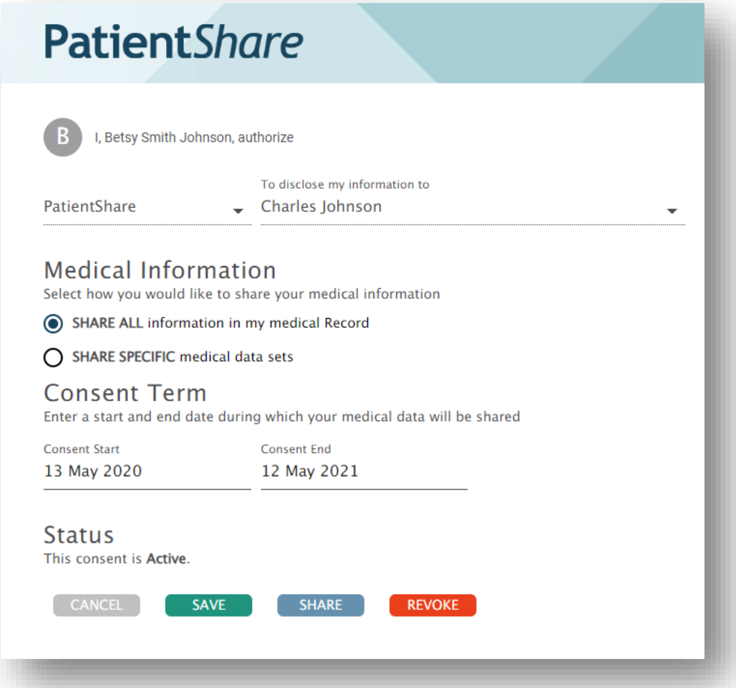
Enter a start and end date during which your medical data will be shared

Consent Start: 13 May 2020

Consent End: 12 May 2021

Status

This consent is **Active**.



PatientShare

I, Betsy Smith Johnson, authorize

PatientShare

To disclose my information to: Charles Johnson

Medical Information

Select how you would like to share your medical information

● SHARE ALL information in my medical Record

○ SHARE SPECIFIC medical data sets

Consent Term

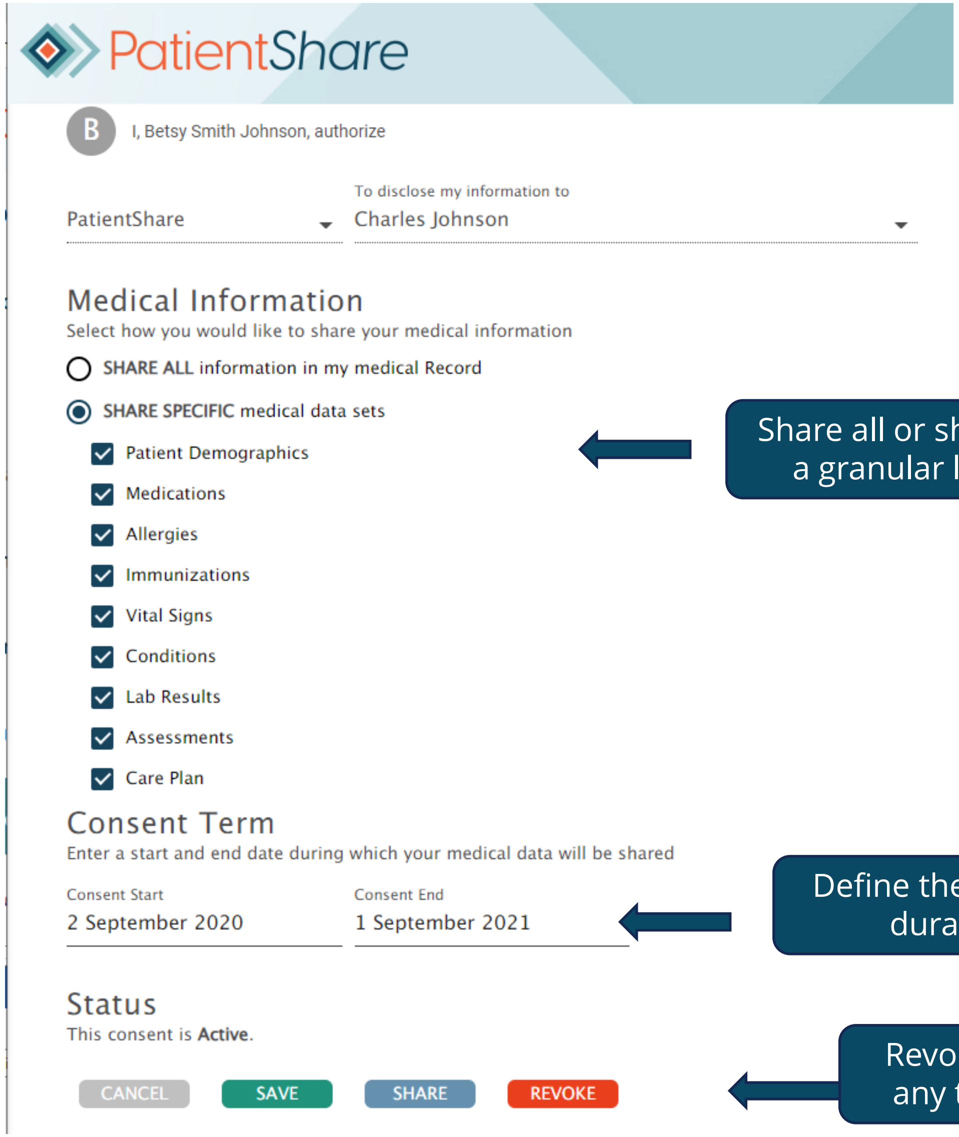
Enter a start and end date during which your medical data will be shared

Consent Start: 13 May 2020

Consent End: 12 May 2021

Status

This consent is **Active**.



PatientShare

I, Betsy Smith Johnson, authorize

PatientShare

To disclose my information to: Charles Johnson

Medical Information

Select how you would like to share your medical information

○ SHARE ALL information in my medical Record

● SHARE SPECIFIC medical data sets

- ☑ Patient Demographics
- ☑ Medications
- ☑ Allergies
- ☑ Immunizations
- ☑ Vital Signs
- ☑ Conditions
- ☑ Lab Results
- ☑ Assessments
- ☑ Care Plan

Consent Term

Enter a start and end date during which your medical data will be shared

Consent Start: 2 September 2020

Consent End: 1 September 2021

Status

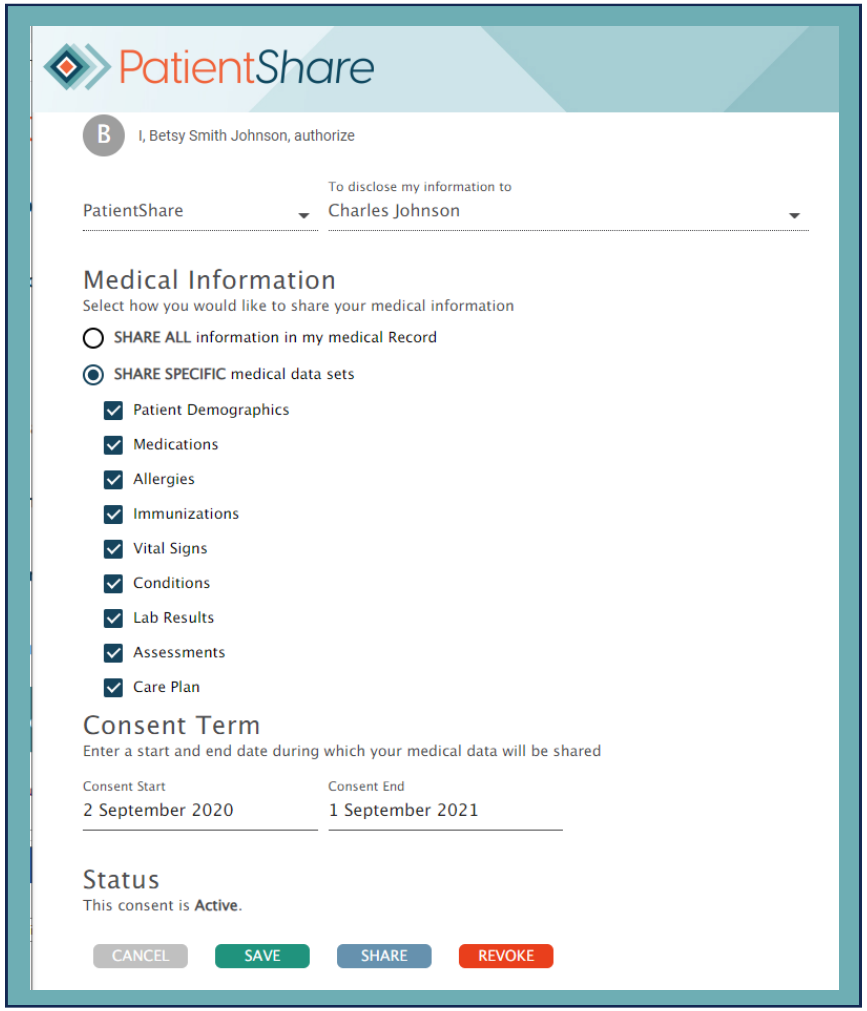
This consent is **Active**.

Share all or share at a granular level

Define the consent duration

Revoke at any time

Sharing Paradigms



PatientShare

B I, Betsy Smith Johnson, authorize

PatientShare

To disclose my information to
Charles Johnson

Medical Information

Select how you would like to share your medical information

○ SHARE ALL information in my medical Record

● SHARE SPECIFIC medical data sets

- ☑ Patient Demographics
- ☑ Medications
- ☑ Allergies
- ☑ Immunizations
- ☑ Vital Signs
- ☑ Conditions
- ☑ Lab Results
- ☑ Assessments
- ☑ Care Plan

Consent Term

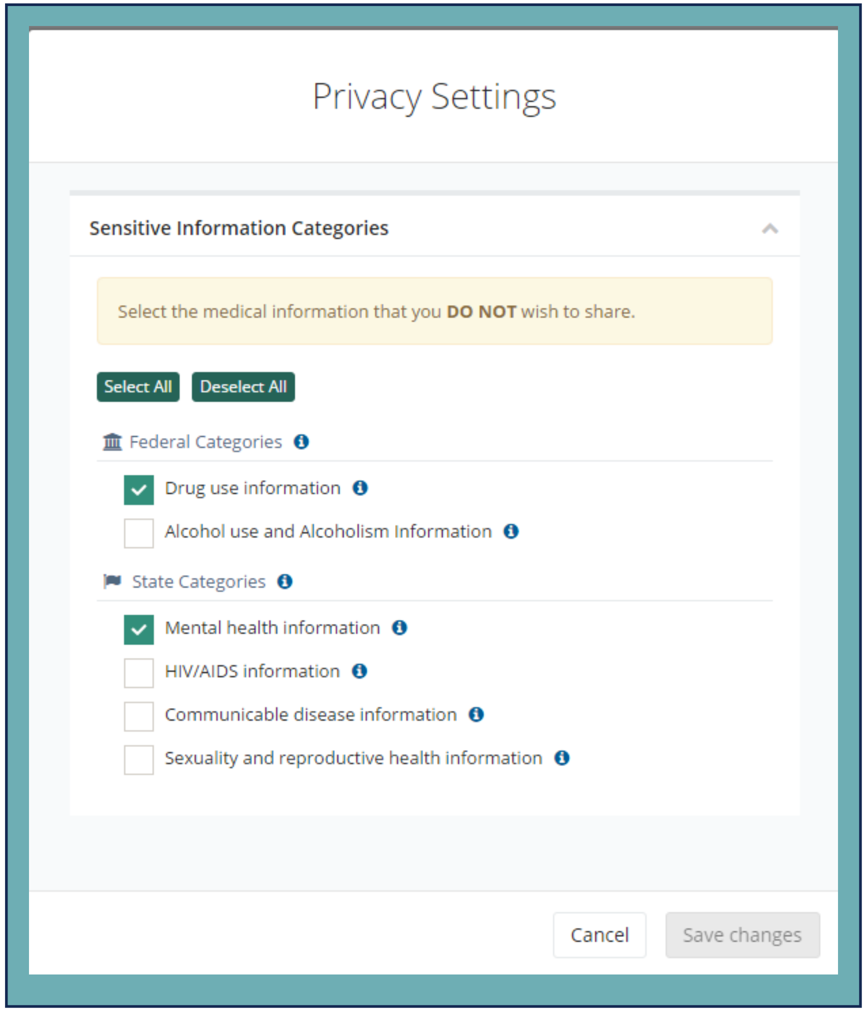
Enter a start and end date during which your medical data will be shared

Consent Start
2 September 2020

Consent End
1 September 2021

Status

This consent is **Active**.



Privacy Settings

Sensitive Information Categories

Select the medical information that you **DO NOT** wish to share.

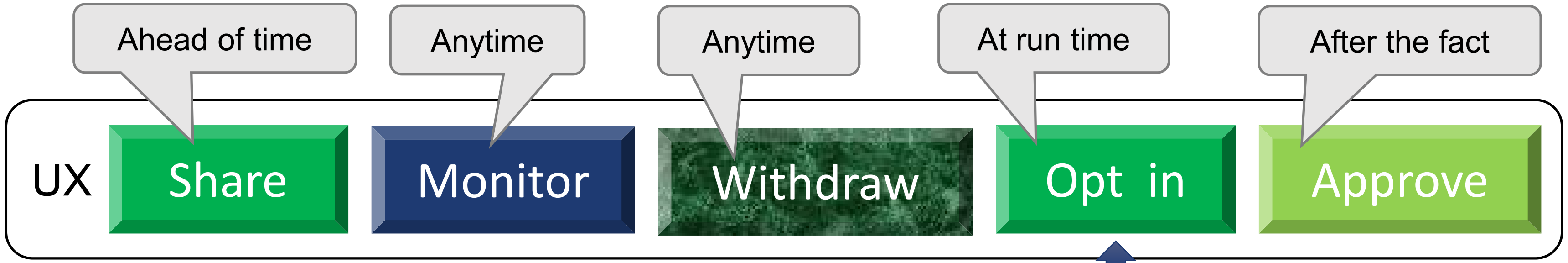
Federal Categories

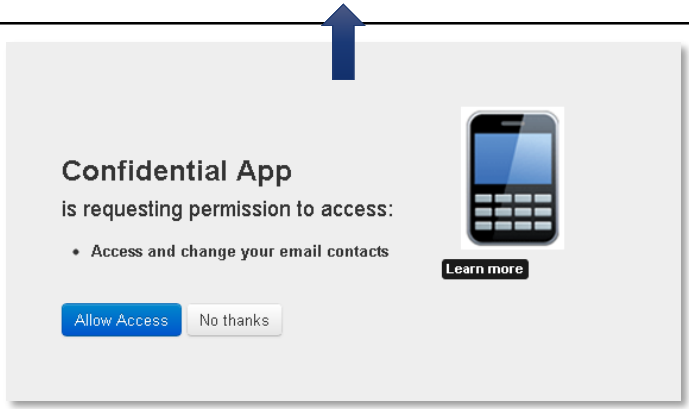
- ☑ Drug use information
- □ Alcohol use and Alcoholism Information

State Categories

- ☑ Mental health information
- □ HIV/AIDS information
- □ Communicable disease information
- □ Sexuality and reproductive health information

UMA user experience opportunities



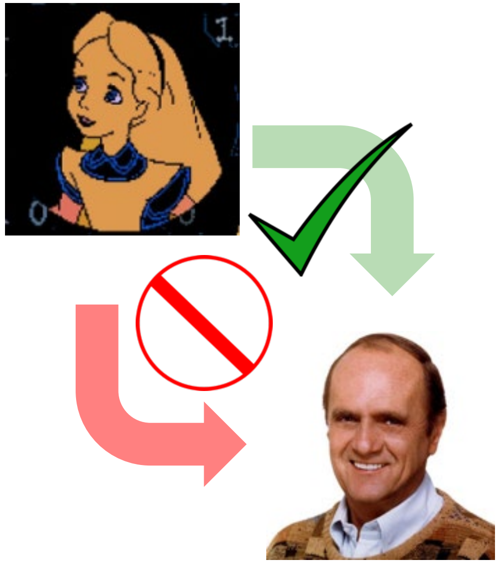

Confidential App

is requesting permission to access:

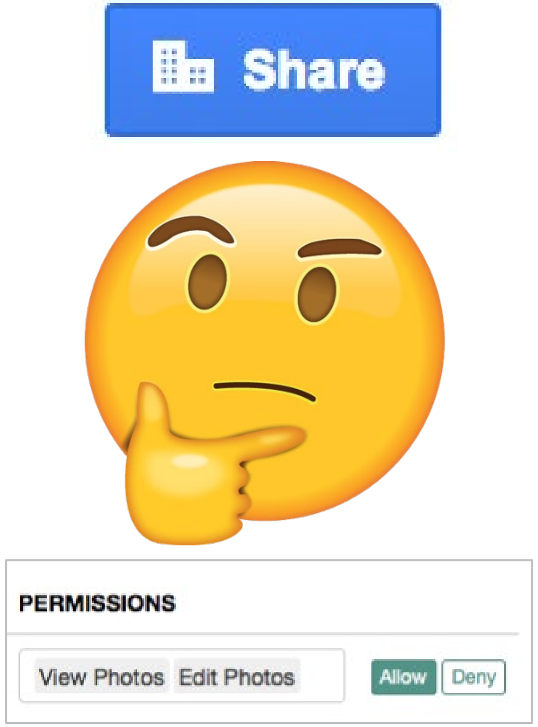
- Access and change your email contacts

Benefits for individuals: a summary

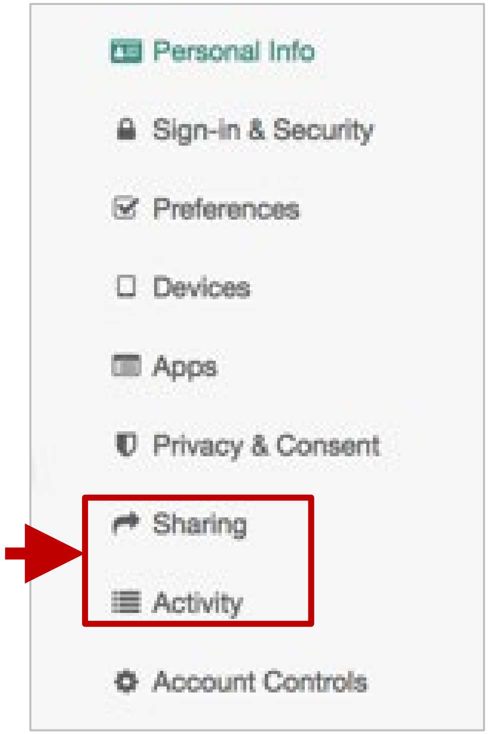
Choice in sharing with other parties



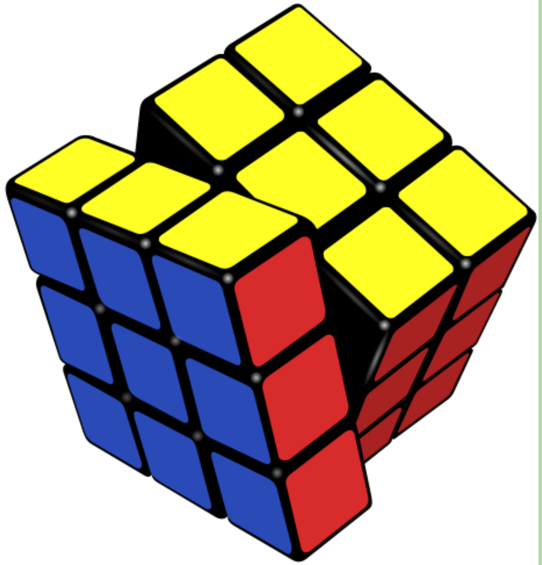
Convenient sharing/approval with no outside influence



Centralizable monitoring and management



Control of who/what/how at a fine grain



Questions?

Patient Centric Solutions, Inc
Nancy Lush

Nlush@PatientCentricSolutions.com
401-965-9347

28 Narragansett Ave
Jamestown, RI 02835

Resources

- HEART WG Home Page
- ONC HEART Webinar Slides
- ONC HEART Webinar
- UMA Implementations

PatientCentricSolutions.com/resources

Consent Model for the Exchange of SDOH Information

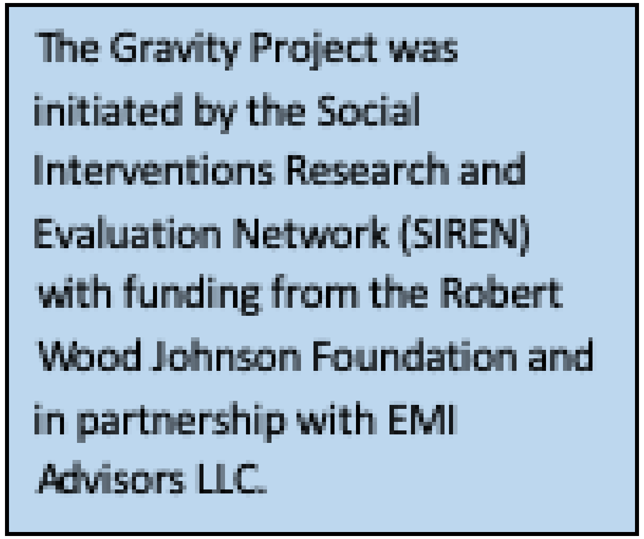
Gravity Project

Robert Dieterle

Technical Director, Gravity Project
CEO, EnableCare LLC

Project Scope

In May 2019, the Gravity Project was launched as a multi-stakeholder public collaborative with the goal to develop, test, and validate standardized SDOH data for use in patient care, care coordination between health and human services sectors, population health management, public health, value-based payment, and clinical research.


The Gravity Project was initiated by the Social Interventions Research and Evaluation Network (SIREN) with funding from the Robert Wood Johnson Foundation and in partnership with EMI Advisors LLC.

Gravity Project Scope: Develop data standards to represent patient level SDOH data documented across four clinical activities: screening, assessment/diagnosis, goal setting, and treatment/interventions.

https://confluence.hl7.org/display/GRAV/The+Gravity+Project

HL7® FHIR® Accelerator Program

- Designed to assist implementers across the health care spectrum in the creation of FHIR Implementation Guides or other informative documents
- Gravity Project became an official Accelerator in August 2019:

http://www.hl7.org/documentcenter/public_temp_3840821C-1C23-BA17-0C64E3ACBE05D630/pressreleases/HL7_PRESS_20190820.pdf

HL7® FHIR® ARGONAUT PROJECT

carin
Creating Access to Real-time Information Now through Consumer-Directed Exchange

CodeX™
Common Oncology Data Elements eXtensions

DA VINCI HL7 FHIR

gravity PROJECT

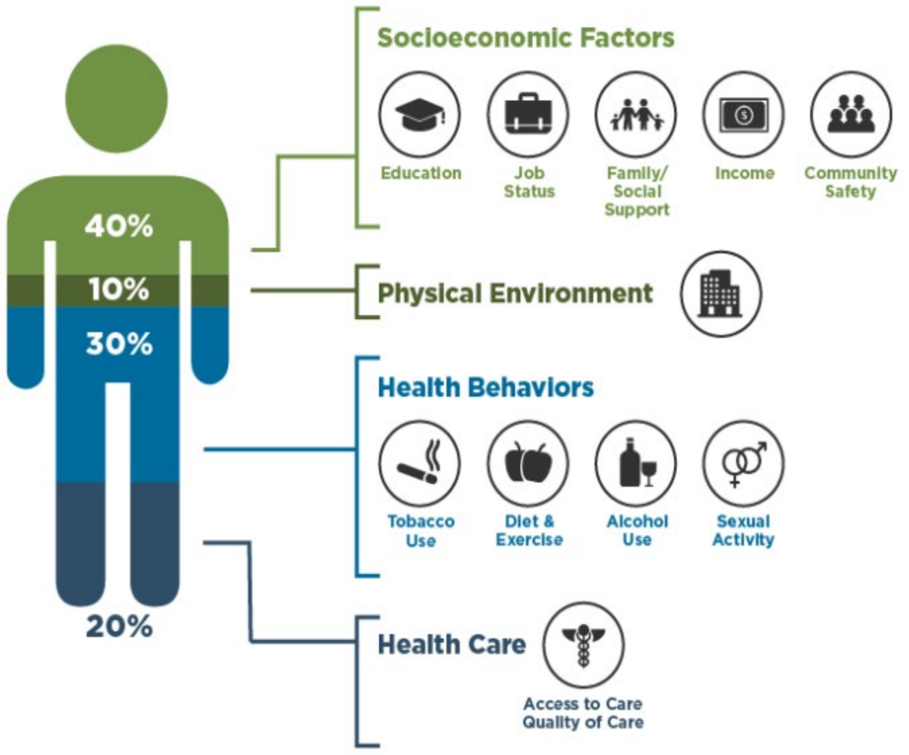
Why are SDOH Important?

There is broad consensus that SDOH information improves whole person care and lowers cost. Unmet social needs negatively impact health outcomes.

Examples

- **Food insecurity** correlates to higher levels of diabetes, hypertension, and heart failure.
- **Housing instability** factors into lower treatment adherence.
- **Transportation barriers** result in missed appointments, delayed care, and lower medication compliance

What Goes Into Your Health?



Source: Institute for Clinical Systems Improvement, Going Beyond Clinical Walls: Solving Complex Problems (October 2014)

Adapted from The Bridgespan Group

Project Founders, Grants, and In-Kind Support

Robert Wood Johnson Foundation

The University of Vermont
LARNER COLLEGE OF MEDICINE

Yale School of Nursing

sirenUCSF

BlueCross BlueShield Association

eat right. Academy of Nutrition and Dietetics

GUIDEWELL

AAFP

KAISER PERMANENTE®

AMA

AHRQ

UnitedHealthcare®

AmeriHealth Caritas

NC

Arkansas

HIGHMARK®

onyx

ASSOCIATION OF AMERICA
ctaa
COMMUNITY TRANSPORTATION

The Office of the National Coordinator for
Health Information Technology

juxly®

blue california

CyncHealth

Humana.

CHILDREN'S HealthWatch

lyft

California Health Care Foundation
HEALTH CARE THAT WORKS FOR ALL CALIFORNIANS

HL7 International

https://confluence.hl7.org/display/GRAV/Gravity+Project+Sponsors

gravity PROJECT®

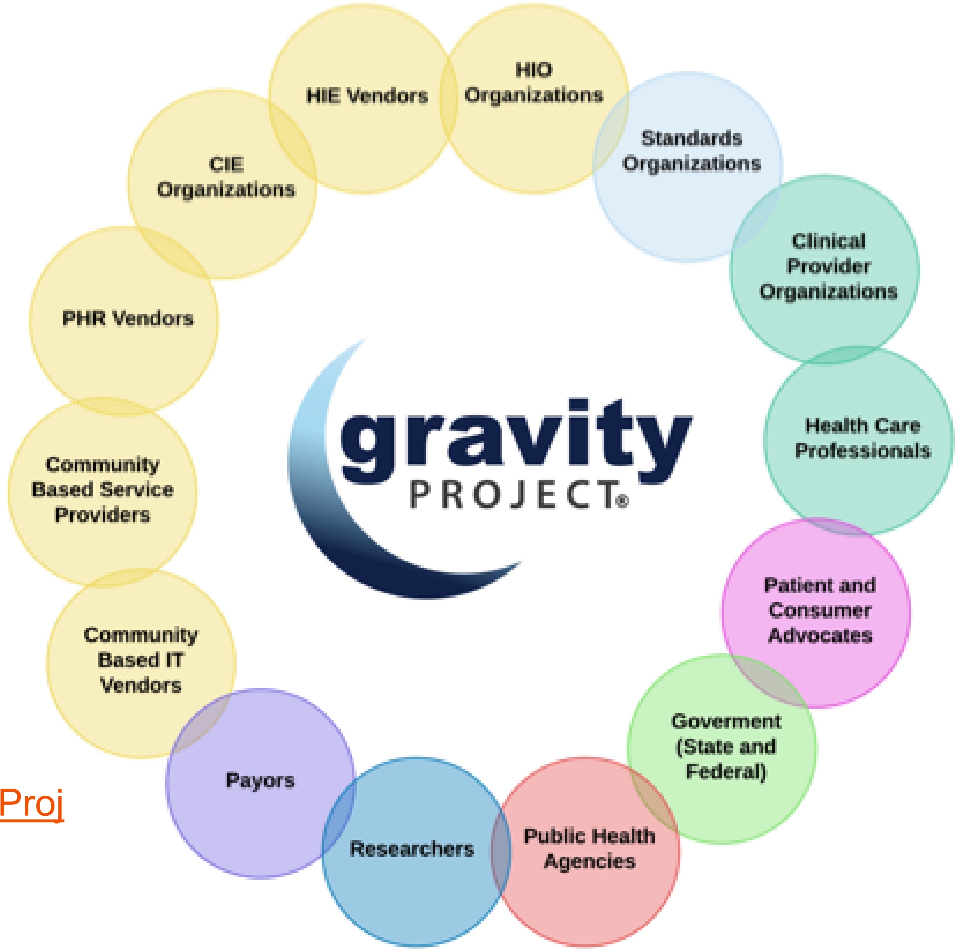
Public Collaboration

Gravity has convened over **1,800+** participants from across the health and human services ecosystem:

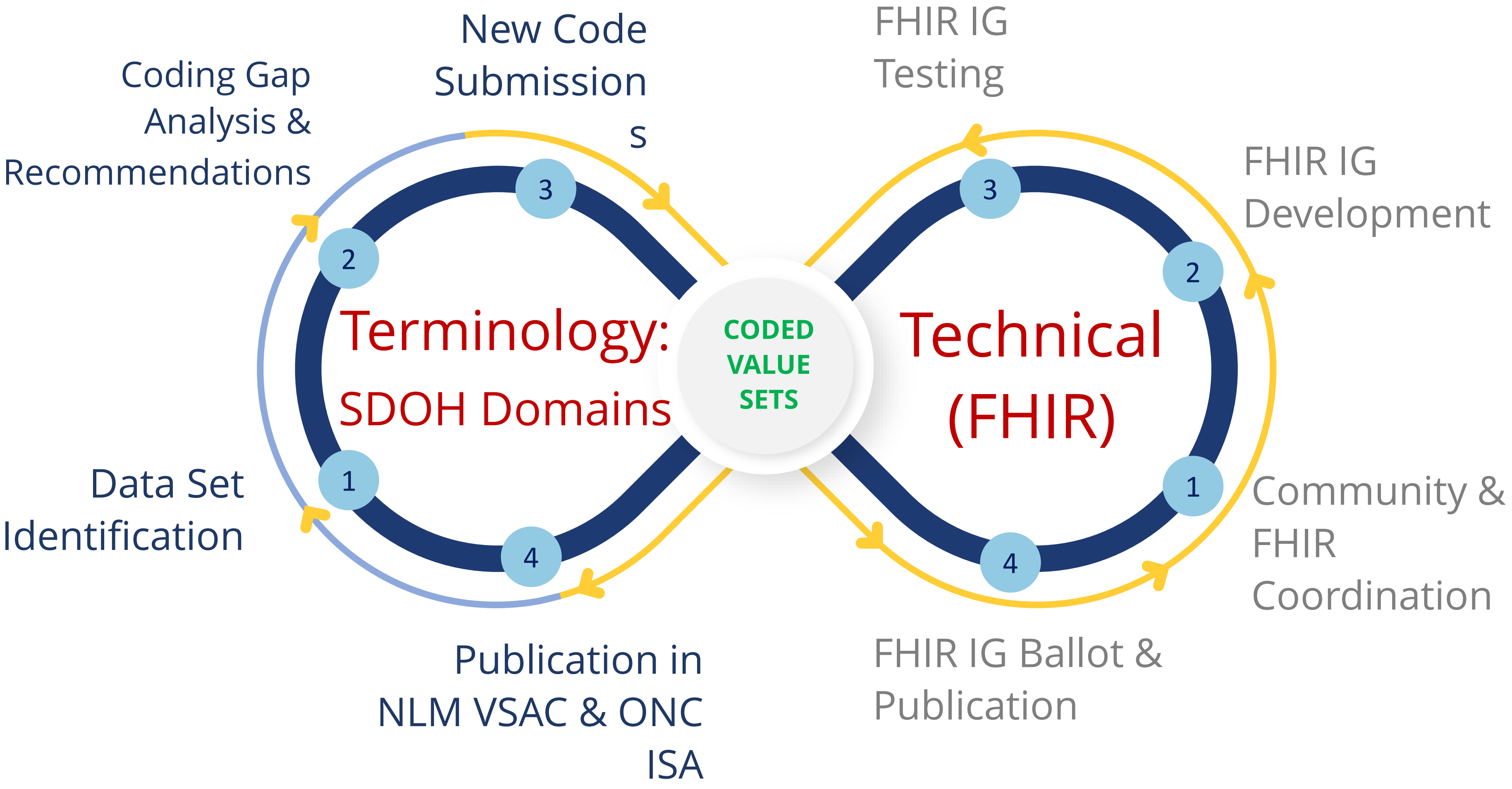
- clinical provider groups
- community-based organizations
- standards development organizations
- federal and state government
- payers
- technology vendors

Terminology Public Calls 4-5:30 pm EST every other Thursday
https://confluence.hl7.org/pages/viewpage.action?pageId=46892669#JointheGravityProject-GravityProjectMembershipList

Technical (FHIR IG) Calls 3-4 pm EST every Wednesday
https://confluence.hl7.org/display/GRAV/FHIR+IG+Work+Group+Meetings


HIE Vendors
HIO Organizations
Standards Organizations
Clinical Provider Organizations
Health Care Professionals
Patient and Consumer Advocates
Goverment (State and Federal)
Public Health Agencies
Researchers
Payors
Community Based IT Vendors
Community Based Service Providers
PHR Vendors
CIE Organizations
gravity PROJECT

Integration of Two Work Streams



Gravity Program Management Office Team

- **Evelyn Gallego,** Program Manager, EMI Advisors
- **Carrie Lousberg**, Project Manager, EMI Advisors
- **Mark Savage,** SDOH Policy Lead**,** USCF/SIREN
- **Sarah DeSilvey,** Clinical Informatics Director, University of Vermont
- **Bob Dieterle,** Technical Director, EnableCare

Technical Workstream

Technical Stream – SDOH Clinical Care FHIR Implementation Guide

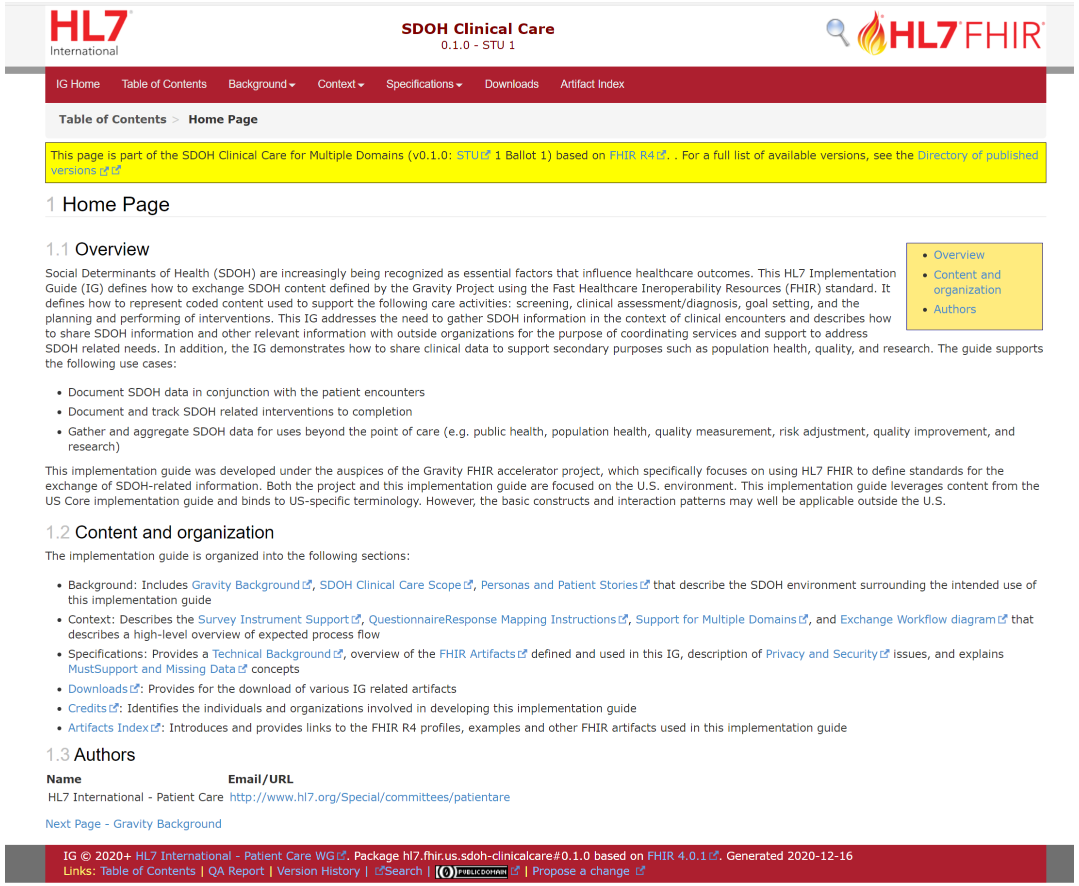
The Office of the National Coordinator for Health Information Technology

1. The SDOH Clinical Care IG is a framework Implementation Guide (IG) and supports multiple domains

2. The IG supports the following clinical activities
   - Assessments
   - Health Concerns / Problems
   - Goals
   - Referrals
   - Consent
   - Aggregation for exchange/reporting

3. Balloted January 2021 as a Standard for Trial Use Level 1 (STU1)

http://hl7.org/fhir/us/sdoh-clinicalcare/2021Jan/



This page is part of the SDOH Clinical Care for Multiple Domains (v0.1.0: STU 1 Ballot 1) based on FHIR R4. . For a full list of available versions, see the Directory of published versions

1 Home Page

1.1 Overview

- Overview
- Content and organization
- Authors

Social Determinants of Health (SDOH) are increasingly being recognized as essential factors that influence healthcare outcomes. This HL7 Implementation Guide (IG) defines how to exchange SDOH content defined by the Gravity Project using the Fast Healthcare Ineroperability Resources (FHIR) standard. It defines how to represent coded content used to support the following care activities: screening, clinical assessment/diagnosis, goal setting, and the planning and performing of interventions. This IG addresses the need to gather SDOH information in the context of clinical encounters and describes how to share SDOH information and other relevant information with outside organizations for the purpose of coordinating services and support to address SDOH related needs. In addition, the IG demonstrates how to share clinical data to support secondary purposes such as population health, quality, and research. The guide supports the following use cases:

- Document SDOH data in conjunction with the patient encounters
- Document and track SDOH related interventions to completion
- Gather and aggregate SDOH data for uses beyond the point of care (e.g. public health, population health, quality measurement, risk adjustment, quality improvement, and research)

This implementation guide was developed under the auspices of the Gravity FHIR accelerator project, which specifically focuses on using HL7 FHIR to define standards for the exchange of SDOH-related information. Both the project and this implementation guide are focused on the U.S. environment. This implementation guide leverages content from the US Core implementation guide and binds to US-specific terminology. However, the basic constructs and interaction patterns may well be applicable outside the U.S.

1.2 Content and organization

The implementation guide is organized into the following sections:

- Background: Includes Gravity Background, SDOH Clinical Care Scope, Personas and Patient Stories that describe the SDOH environment surrounding the intended use of this implementation guide
- Context: Describes the Survey Instrument Support, QuestionnaireResponse Mapping Instructions, Support for Multiple Domains, and Exchange Workflow diagram that describes a high-level overview of expected process flow
- Specifications: Provides a Technical Background, overview of the FHIR Artifacts defined and used in this IG, description of Privacy and Security issues, and explains MustSupport and Missing Data concepts
- Downloads: Provides for the download of various IG related artifacts
- Credits: Identifies the individuals and organizations involved in developing this implementation guide
- Artifacts Index: Introduces and provides links to the FHIR R4 profiles, examples and other FHIR artifacts used in this implementation guide

1.3 Authors

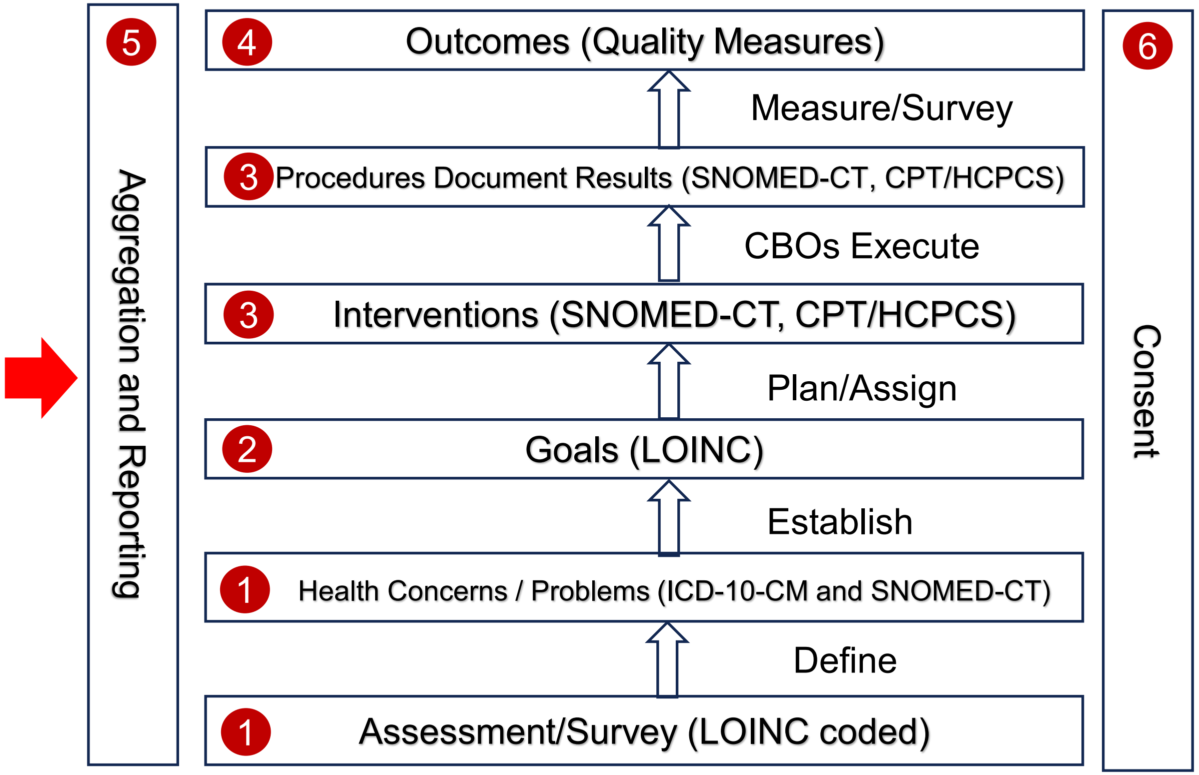
Name	Email/URL
HL7 International - Patient Care	http://www.hl7.org/Special/committees/patientare

Next Page - Gravity Background

IG © 2020+ HL7 International - Patient Care WG. Package hl7.fhir.us.sdoh-clinicalcare#0.1.0 based on FHIR 4.0.1. Generated 2020-12-16
Links: Table of Contents | QA Report | Version History | Search | PUBLIC DOMAIN | Propose a change

Gravity FHIR SDOH Clinical Care IG Scope

1. Document SDOH data in conjunction with the patient encounter and define Health Concerns / Problems.
2. Patient and provider establish SDOH related goals.
3. Plan, communicate, and track related interventions to completion.
4. Measure outcomes.
5. Establish cohorts of patients with common SDOH characteristics for uses beyond the point of care (e.g., population health management, quality reporting, and risk adjustment/ risk stratification).
6. Manage patient consent



5 Aggregation and Reporting

4 Outcomes (Quality Measures)

Measure/Survey

3 Procedures Document Results (SNOMED-CT, CPT/HCPCS)

CBOs Execute

3 Interventions (SNOMED-CT, CPT/HCPCS)

Plan/Assign

2 Goals (LOINC)

Establish

1 Health Concerns / Problems (ICD-10-CM and SNOMED-CT)

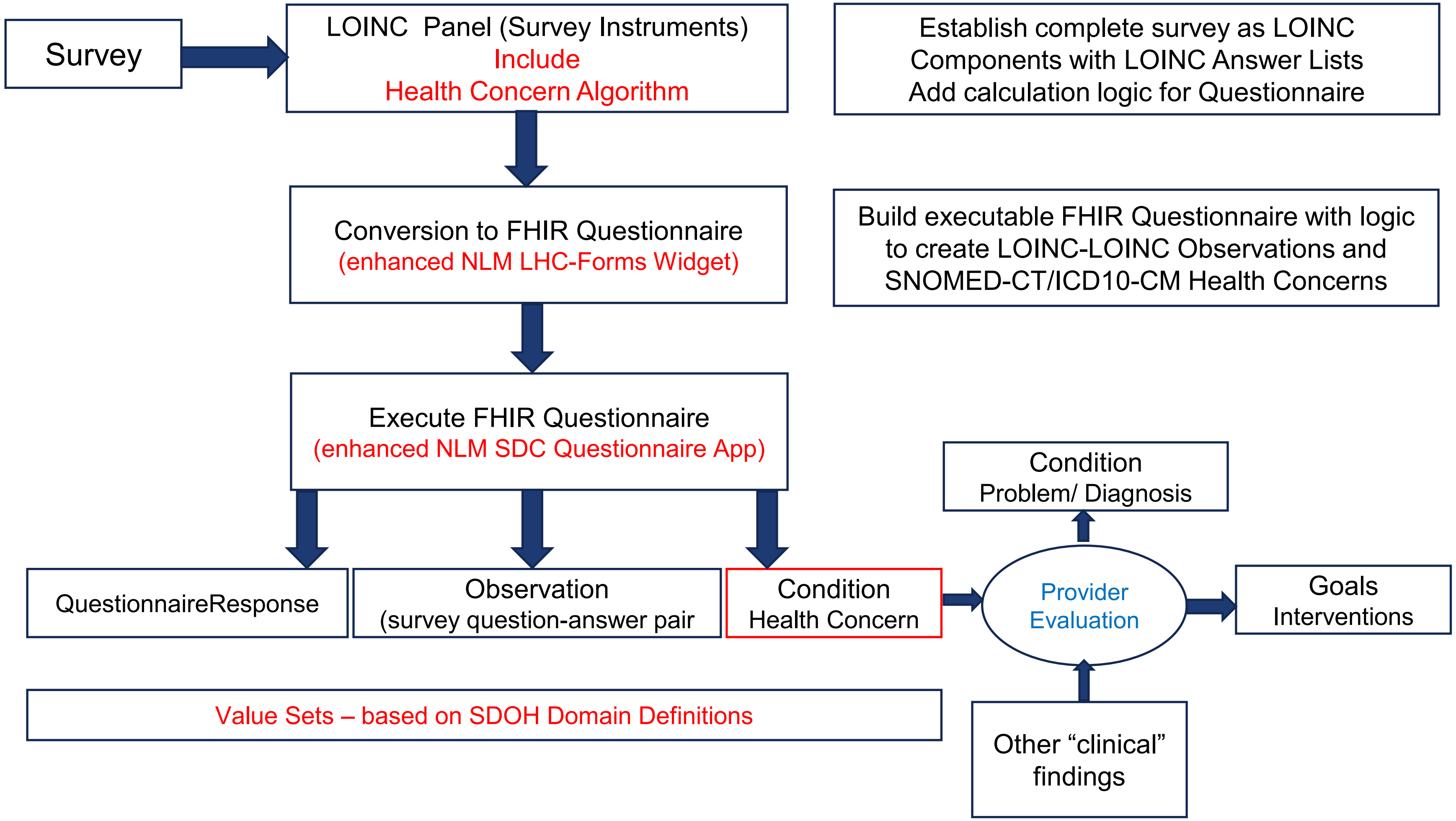
Define

1 Assessment/Survey (LOINC coded)

6 Consent

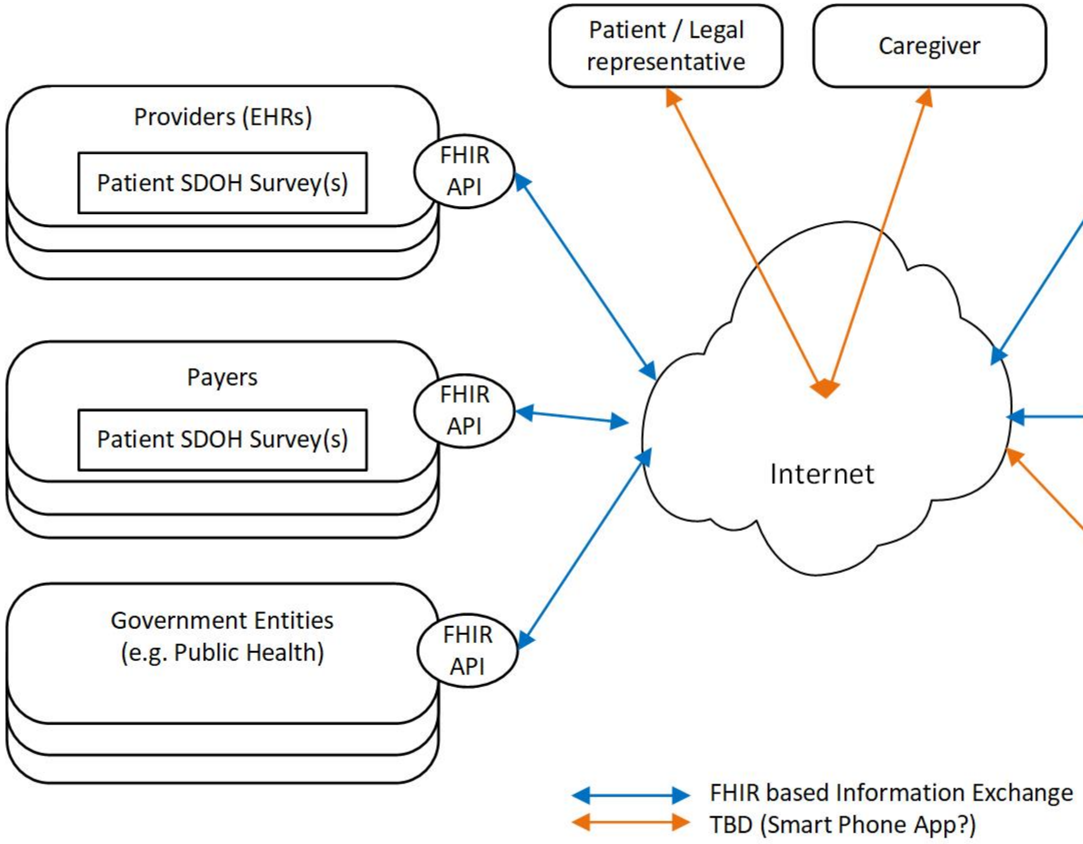
http://build.fhir.org/ig/HL7/fhir-sdoh-clinicalcare/

Enabling Survey Instruments


Survey
LOINC Panel (Survey Instruments)
Include
Health Concern Algorithm
Establish complete survey as LOINC Components with LOINC Answer Lists
Add calculation logic for Questionnaire
Conversion to FHIR Questionnaire
(enhanced NLM LHC-Forms Widget)
Build executable FHIR Questionnaire with logic to create LOINC-LOINC Observations and SNOMED-CT/ICD10-CM Health Concerns
Execute FHIR Questionnaire
(enhanced NLM SDC Questionnaire App)
Condition
Problem/ Diagnosis
QuestionnaireResponse
Observation
(survey question-answer pair
Condition
Health Concern
Provider
Evaluation
Goals
Interventions
Value Sets – based on SDOH Domain Definitions
Other "clinical" findings

Note: all Survey instruments produce Health Concerns with Gravity defined value sets

Interactions between SDOH participants


Patient / Legal representative
Caregiver
Providers (EHRs)
Patient SDOH Survey(s)
FHIR API
Payers
Patient SDOH Survey(s)
FHIR API
Government Entities (e.g. Public Health)
FHIR API
Internet
Coordination Platform (CP)
Patient SDOH Survey(s)
FHIR API
Community Based Organization (CBO)
FHIR API
Community Based Organization (CBO)
FHIR based Information Exchange
TBD (Smart Phone App?)

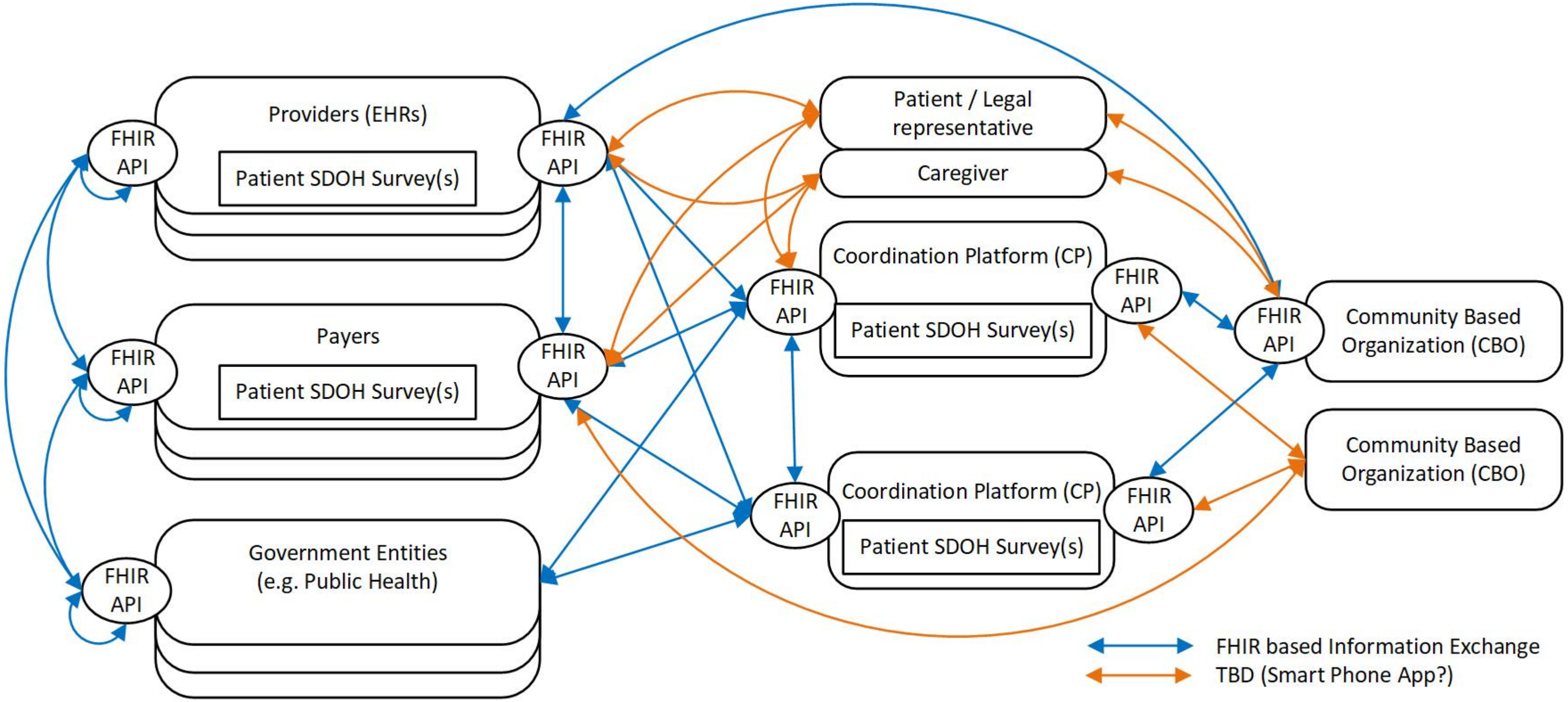
Coordination Platform (CP) – Typically CPs are based on a referral platforms such as UniteUs, Aunt Bertha, NowPow, 211 (this is not an exhaustive list)

Community Based Organizations (CBO) -- Typically CBOs provide the services to address social risk and need (e.g. food pantry)

Both CPs and CBOs may provide a number of services that overlap and differ substantially by community.

Interaction with a patient or caregiver may required alternative methods if internet access is not available

Detailed Exchanges Supported by the SDOH FHIR IG


Providers (EHRs)
Patient SDOH Survey(s)
FHIR API
FHIR API
Payers
Patient SDOH Survey(s)
FHIR API
FHIR API
Government Entities (e.g. Public Health)
FHIR API
Patient / Legal representative
Caregiver
Coordination Platform (CP)
FHIR API
Patient SDOH Survey(s)
FHIR API
Coordination Platform (CP)
FHIR API
Patient SDOH Survey(s)
FHIR API
FHIR API
Community Based Organization (CBO)
Community Based Organization (CBO)
FHIR based Information Exchange
TBD (Smart Phone App?)

Note: Where two FHIR APIs are shown, it is for drawing simplicity and not a technical requirement

Addressing Sensitive Data and Consent in SDOH

Examples of sensitive SDOH data

- Clearly sensitive data
  - Spousal abuse
  - Immigration Status
- Frequently sensitive data
  - Homelessness
  - Employment
- Less obviously sensitive data
  - Home address
  - Telephone number

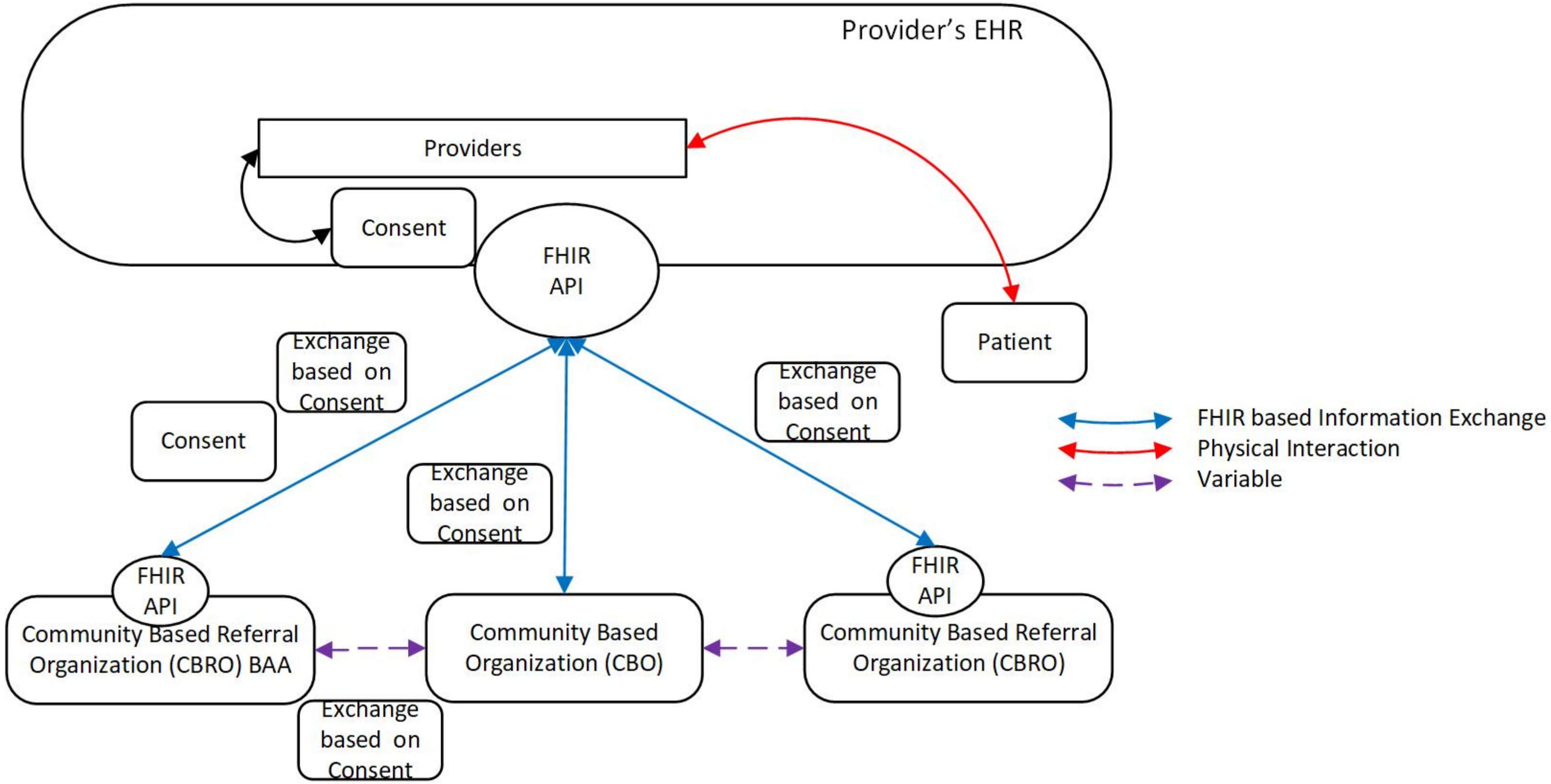
Examples of specific consent

- Will not share sensitive data with anyone
- Will share sensitive data with:
  - Specific individuals/organizations
  - Protections regarding rerelease of the information
- Will share specific data with specific organizations for purpose of referrals/interventions
- Will not share data with specific organizations due to lack of trust or experience
- I want to revoke an existing consent

Protections afforded personal information

- HIPAA – defines covered entities and Personal Health Information (PHI)
  - Allowed exchanges to covered entities defined by Treatment, Payment and Operations (TPO)
  - requires patient consent to release beyond the covered entitles or TPO
- Federal regulations – e.g. 42 CFR Part 2 (protection for information regarding federally funded substance abuse centers)
- State regulations – varied based on specific state regulations

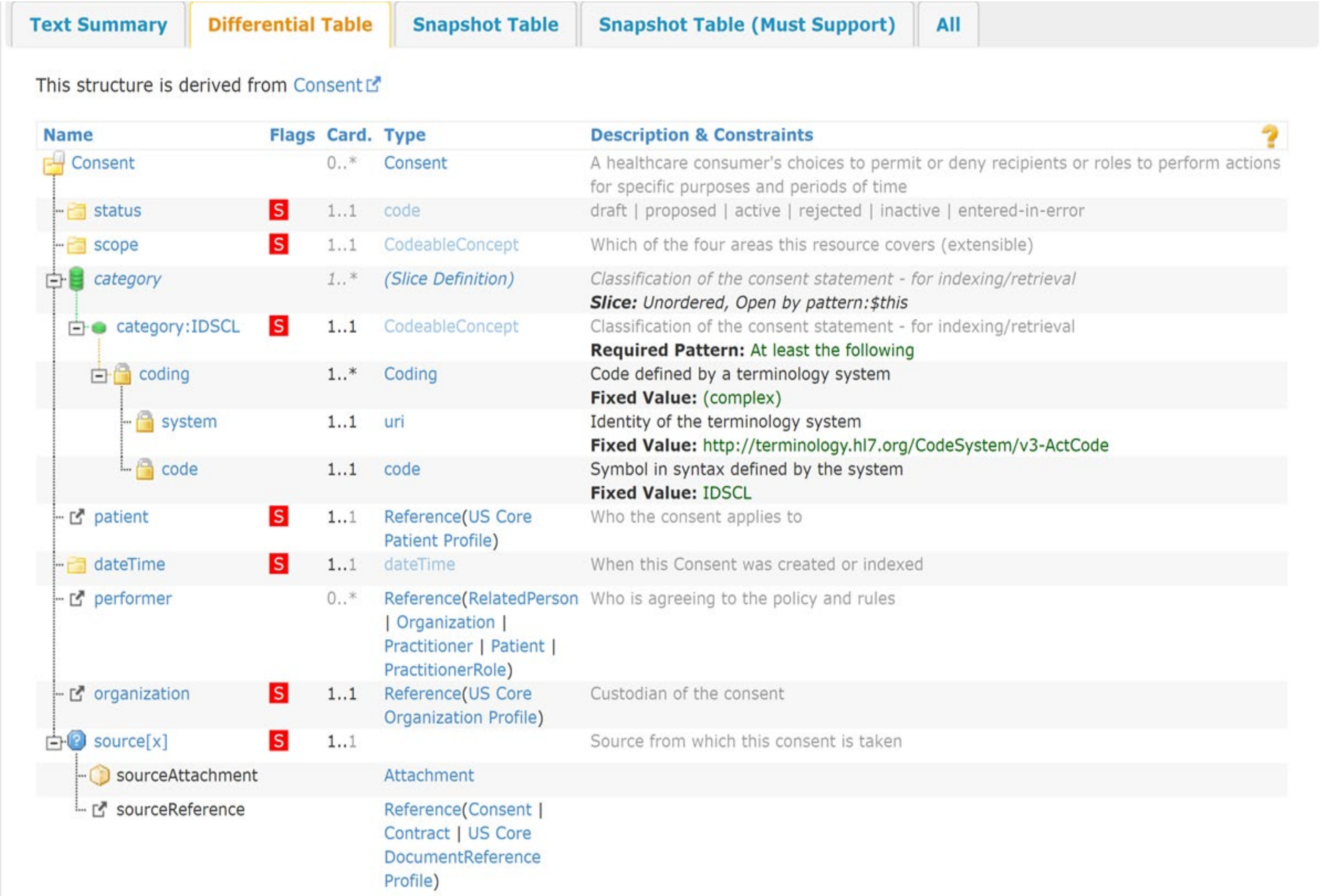
Consent exchange for SDOH Clinical Care IG


Provider's EHR
Providers
Consent
FHIR API
Patient
Exchange based on Consent
Consent
Exchange based on Consent
Exchange based on Consent
FHIR API
Community Based Referral Organization (CBRO) BAA
Community Based Organization (CBO)
FHIR API
Community Based Referral Organization (CBRO)
Exchange based on Consent
FHIR based Information Exchange
Physical Interaction
Variable

SDOH Clinical Care IG – Consent Profile

- We are in the process of ballot reconciliation and the Consent profile may change based on ballot comments and experience from the May Connectathon

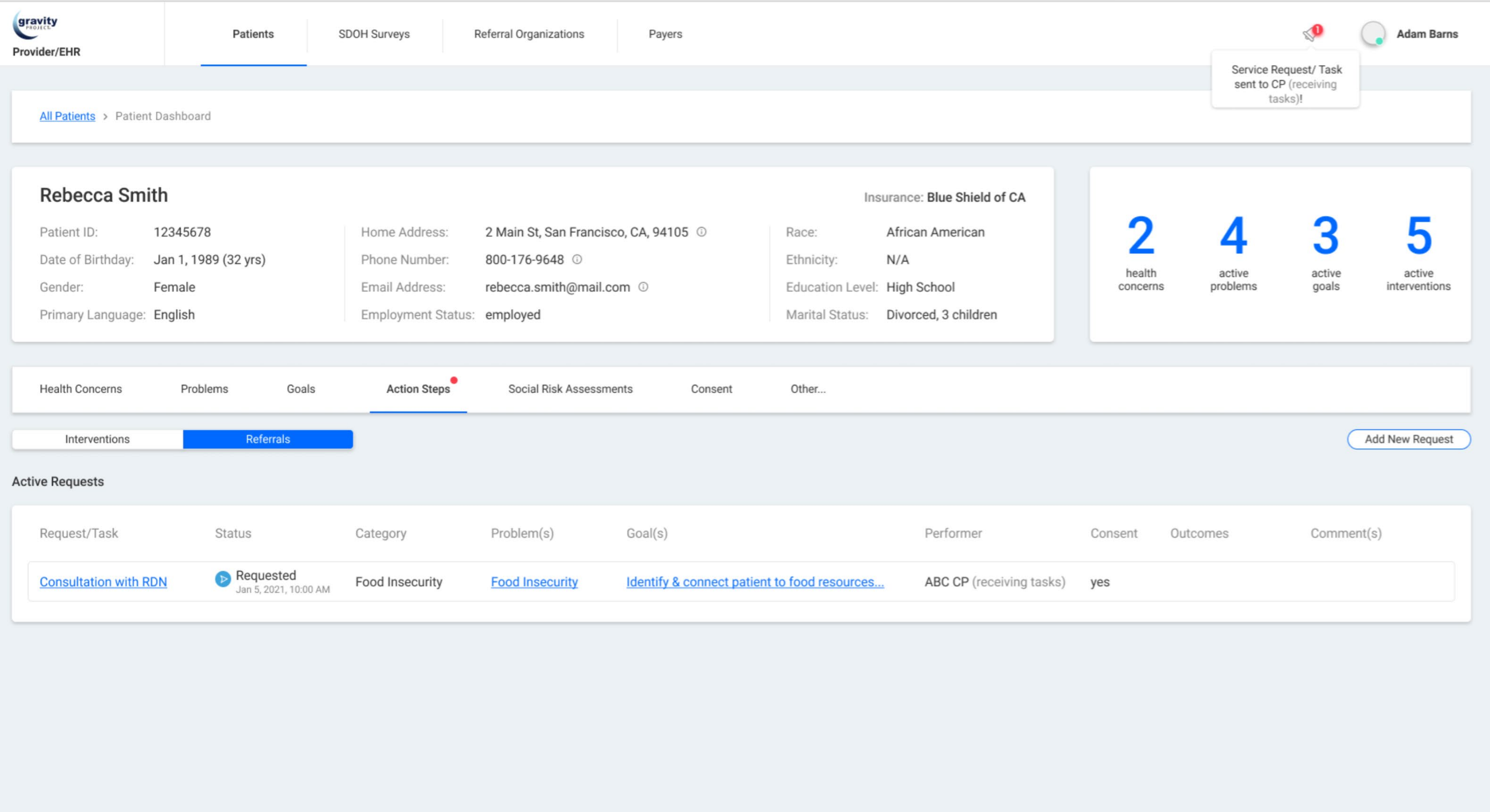
- Used to exchange the patients consent to release information to a community-based referral organization under a BAA with the covered entity (referenced by the ServiceRequest)



This structure is derived from Consent

Name	Flags	Card.	Type	Description & Constraints
Consent		0..*	Consent	A healthcare consumer's choices to permit or deny recipients or roles to perform actions for specific purposes and periods of time
status	S	1..1	code	draft | proposed | active | rejected | inactive | entered-in-error
scope	S	1..1	CodeableConcept	Which of the four areas this resource covers (extensible)
category		*1..**	*(Slice Definition)*	*Classification of the consent statement - for indexing/retrieval* ***Slice:*** *Unordered, Open by pattern:$this*
category:IDSCL	S	1..1	CodeableConcept	Classification of the consent statement - for indexing/retrieval **Required Pattern:** At least the following
coding		1..*	Coding	Code defined by a terminology system **Fixed Value:** (complex)
system		1..1	uri	Identity of the terminology system **Fixed Value:** http://terminology.hl7.org/CodeSystem/v3-ActCode
code		1..1	code	Symbol in syntax defined by the system **Fixed Value:** IDSCL
patient	S	1..1	Reference(US Core Patient Profile)	Who the consent applies to
dateTime	S	1..1	dateTime	When this Consent was created or indexed
performer		0..*	Reference(RelatedPerson | Organization | Practitioner | Patient | PractitionerRole)	Who is agreeing to the policy and rules
organization	S	1..1	Reference(US Core Organization Profile)	Custodian of the consent
source[x]	S	1..1		Source from which this consent is taken
sourceAttachment			Attachment	
sourceReference			Reference(Consent | Contract | US Core DocumentReference Profile)	

Prototype for the SDOH FHIR IG Reference Implementation



Service Request/ Task sent to CP (receiving tasks)!

All Patients › Patient Dashboard

Rebecca Smith

Insurance: Blue Shield of CA

Patient ID: 12345678
Date of Birthday: Jan 1, 1989 (32 yrs)
Gender: Female
Primary Language: English

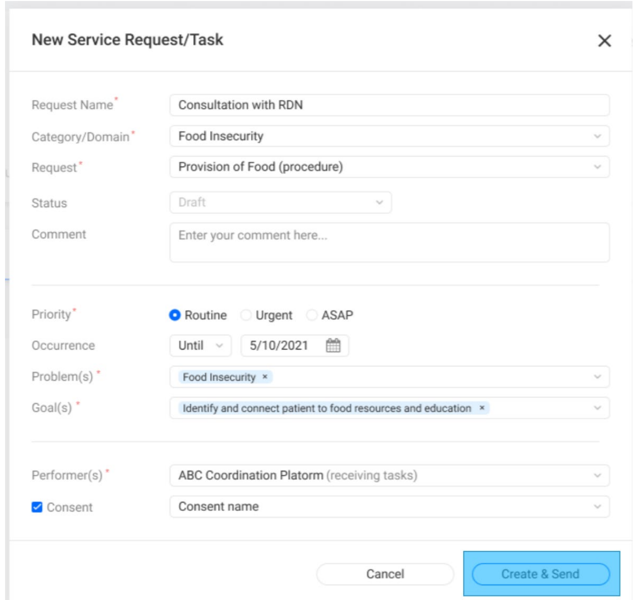
Home Address: 2 Main St, San Francisco, CA, 94105
Phone Number: 800-176-9648
Email Address: rebecca.smith@mail.com
Employment Status: employed

Race: African American
Ethnicity: N/A
Education Level: High School
Marital Status: Divorced, 3 children

2 health concerns
4 active problems
3 active goals
5 active interventions

Active Requests

Request/Task	Status	Category	Problem(s)	Goal(s)	Performer	Consent	Outcomes	Comment(s)
Consultation with RDN	Requested Jan 5, 2021, 10:00 AM	Food Insecurity	Food Insecurity	Identify & connect patient to food resources...	ABC CP (receiving tasks)	yes		



Request Name*: Consultation with RDN
Category/Domain*: Food Insecurity
Request*: Provision of Food (procedure)
Status: Draft
Comment: Enter your comment here...

Priority*: ● Routine ○ Urgent ○ ASAP
Occurrence: Until 5/10/2021
Problem(s)*: Food Insecurity ×
Goal(s)*: Identify and connect patient to food resources and education ×

Performer(s)*: ABC Coordination Platorm (receiving tasks)
☑ Consent: Consent name

Ongoing HL7 Data Tagging and Consent effort

- Security Workgroup
- Community Based Care and Privacy (CBCP) Workgroup
- Patient Care
- HL7 FHIR R4 Implementation Guides defining Consent Profiles
  - SDOH FHIR IG
  - Bidirectional Services eReferrals (BSeR) FHIR IG

Results from the January SDOH Clinical Care IG Ballot

The Office of the National Coordinator for Health Information Technology

Results of ballot voting

- Affirmative 63
- Negative 30
- Abstain 56
- No Vote 43
- Total 192

The ballot met the **60%** threshold required to publish as an STU

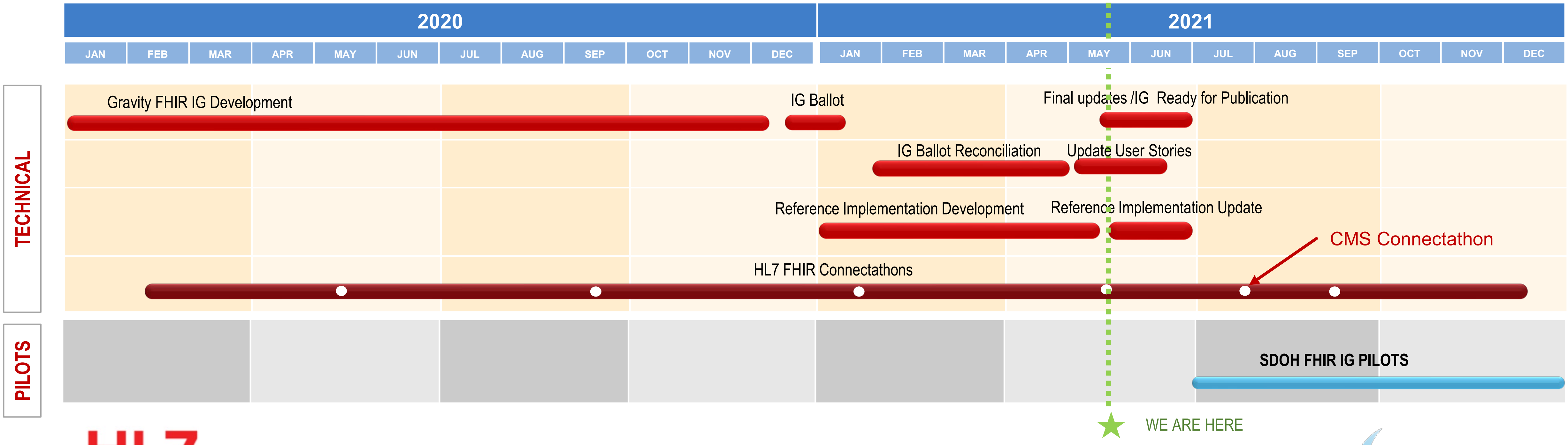
Ballot comments submitted

- Total ballot comments 227
- Total negative comments 72
- Total affirmative comments 155

Note: Affirmative comments include typos, questions, suggestions, comments

Ballot Reconciliation Status

- The ballot reconciliation process started on 2/7/2021 and is expected to continue until the end of April.
- As of 4/30/2021 198 of the 227 ballot comments have dispositions -- 29 to go (all are focused on the patient story)



2020

2021

JAN FEB MAR APR MAY JUN JUL AUG SEP OCT NOV DEC

JAN FEB MAR APR MAY JUN JUL AUG SEP OCT NOV DEC

TECHNICAL

Gravity FHIR IG Development

IG Ballot

Final updates /IG Ready for Publication

IG Ballot Reconciliation

Update User Stories

Reference Implementation Development

Reference Implementation Update

CMS Connectathon

HL7 FHIR Connectathons

PILOTS

SDOH FHIR IG PILOTS

WE ARE HERE

HL7 International

gravity PROJECT

Join our Project!

- Join the Gravity Project: https://confluence.hl7.org/display/GRAV/Join+the+Gravity+Project
  - Public Collaborative Workgroup meets bi-weekly on **Thursdays' 4:00 to 5:30 pm ET**
  - SDOH FHIR IG Workgroup meets weekly on **Weds. 3:00 to 4:00 pm ET**
- Help us find new sponsors and partners
- Join us at the HL7 CMS Connectathon SDOH Track – register at http://www.hl7.org/events/cms/ through July 1, 2021 (watch the Gravity Project Confluence site for signup instructions)
- Submit SDOH domain data elements (especially for Interventions): https://confluence.hl7.org/display/GRAV/Data+Element+Submission
- Help us with Gravity Education & Outreach
  - Social Media handles to share or tag us to relevant information

    @the gravityproj

    - https://www.linkedin.com/company/gravity-project
  - Partner with us on development of blogs, manuscripts, dissemination materials

Questions?

Robert Dieterle

Technical Director, Gravity Project

CEO EnableCare LLC

rdieterle@enablecare.us

Additional questions? Contact: gravityproject@emiadvisors.net

@thegravityproj

https://www.linkedin.com/company/gravity-project

Q&A

Thank you for joining!