Canada Health Infoway
Inforoute Santé du Canada

HALO Working Group Meeting

Meeting Summary

Meeting Chair: Alex Reis			
Date and Time	**Location**	**Note Taker**	**Next Meeting Date**
July 7, 2025,1:00pm – 2:30pm ET	Virtual	Sadrina Petit, Senior Project Analyst, Digital Health Interoperability	July 14, 2025,1:00pm-2:30pm ET
Meeting Agenda: 1. Co- Chair Update 2. Set Context Overview 3. Set Context Deep Dive – In Simplifier 4. Clear Context **5.** Q&A / Collaboration			
Presenters			
• Alex Reis | Director, Digital Health Interoperability, Canada Health Infoway • Colin Kent-Shepherd | Software Architect, Hamilton Health Sciences			
Invited Guests			
Public			

---

1. **Welcome and Introductions**

   A. Reis welcomed all participants to the working group meeting and introduced Colin Kent-Shepherd. Meeting materials and recording of the session will be made available on the InfoCentral working group.

2. **Content Presentation**

   The Infoway team presented each of the agenda items as outlined above. The meeting focused on the set-context and clear-context operations.

   a. Colin explained that Set Context prepopulates the SOFA with FHIR resources and contextual references so SMART apps can launch with the data they need. The operation is invoked via HTTP POST and returns a launch ID along with a transaction response bundle confirming what was loaded.

   b. The clear-context operation was also reviewed; it removes previously loaded resources and contextual references to reset the SOFA state. Let me know if you want this formatted for email or meeting notes.

   Imanma Egeonu accepted the co-chair role and stressed the importance of incorporating vendor perspectives.

The group flagged a security concern: the fhirUser claim in the ID token should come from a trusted identity provider to avoid impersonation or privilege escalation.

The presentation deck is available HALO Working Group Meeting

The video recording is available HALO Working Group Meeting

3. Questions raised during the working group meeting:

How does FHIR Patient/$everything relate to HALO $set-context? Are they interchangeable?

They serve different purposes.

- **$set-context** = *POC writes data + context* into the jurisdictional SOFA **before** launching a SMART app.
- **Patient/$everything** = *SMART app reads data* already in the server **after** launch.
  HALO doesn't require or standardize $everything; implementations may expose it via CapabilityStatement.

If an app requests the launch scope, what's the *minimum* context that should be sent?

Send the current Patient and Encounter (if each is in context in the POC). Include them in the transaction Bundle and set the patient / encounter parameters accordingly.

Can a SMART app be launched without patient or encounter context?

Yes. If the app does **not** request launch (or specific launch/patient, launch/encounter, etc.) scopes, the POC does not need to send Patient/Encounter in $set-context.

How are other in-context resources (e.g., Appointment) indicated?

Use SMART launch hints like launch/Appointment (or another resource type). Include the resource in the Bundle and reference it in the $set-context fhirContext[] parameter.

In the $set-context Parameters, are we mixing clinical data and security/identity fields? Is that safe?

Yes, the payload currently includes both clinical context (patient, encounter, etc.) and **fhirUser**, which is security/identity related. Participants noted this mixing and asked for clearer spec guidance differentiating the two domains.

Because fhirUser becomes an ID token claim (OIDC), is it acceptable for the POC to "inject" it? Shouldn't an Identity Provider supply that claim?

This is an open security concern. Current HALO flow allows the POC to provide a PractitionerRole referenced by fhirUser; the SOFA/Auth layer is expected to validate tokens and crosscheck values. The group agreed that additional guidance (trust model, IdP sourcing, validation rules) is needed and will be addressed in a followup.

Can we specify a Time-to-Live (TTL) for data pushed via $set-context?

Not in the current version. TTL support was suggested and will be evaluated (needs alignment with offline and synchronization scenarios).

What prevents malicious or unauthorized $clear-context calls (e.g., guessing launchIds and deleting data)?

Intended model: The launchId is bound to the authenticated user/session that created the context; only an authorized caller (same user or privileged jurisdictional service) can clear it. The spec will be strengthened to state required authorization checks; implementations should also use high entropy IDs and consider rate limiting.

Commented [AR1]: @Holitska , Magdolna can you verify this Q and A Mag?

Commented [HM2R1]: The answer says that a follow-up is needed, so is that enough to cover this question? This is the email from Aftab we asked for