SMART on FHIR: Will it Change Accountability for Privacy and Security Risks?

Gavin Tong

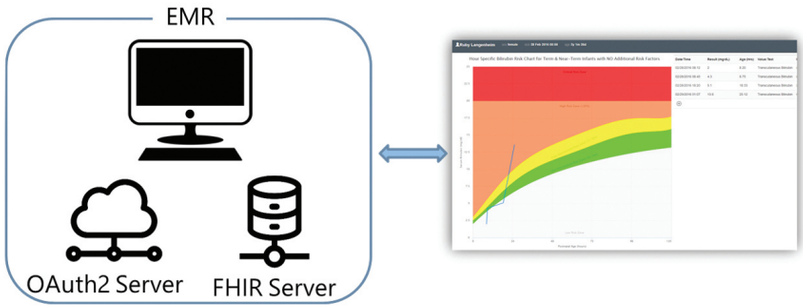
MBA, CPHIMS-CA, Standards and Interoperability Editor, is an Associate Managing Partner with Gevity in Toronto, Ontario

It's becoming increasingly apparent that SMART on FHIR application program interfaces (APIs) will change how we integrate source systems such as EMR and HIS with external applications. As with any new 'technology' in healthcare, it also raises questions about accountabilities for risks related to privacy, security and patient safety.

SMART on FHIR is a specification that describes how an external app (i.e., a SMART app) can query a SMART on FHIR API to get data out of the source system. The basic use case goes something like this: a user of a source system like an EMR can launch a SMART app. The EMR passes some information to the SMART app such as the URL for the EMR's API, which the SMART app can then query to get data from the EMR and do something with it. That 'something' could be just about anything, from presenting a growth chart to calculating a cardiovascular risk score. In theory, the SMART app could even write data back to the source system using the SMART on FHIR API. If you're curious to see some example SMART apps check out https://apps.SMARThealthit.org

The SMART on FHIR specification describes how two major components of the API work: 1) An OAuth2 server which deals with permissions to launch SMART apps, establishing secure connections between the API and SMART apps, and passing patient context from the source system to the SMART app; and 2) a FHIR server which receives the queries and provides the data back to the SMART app using FHIR as the standard for the data structure and syntax.

The traditional approach to integrating source systems with external applications is to force source system vendors to build interfaces and new functionality within their products.



With SMART on FHIR, the vendors can simply declare their SMART on FHIR API and external apps can be the ones that are forced to determine how to change in order to interoperate. There's a number of data standardization considerations that need to be addressed for this to work, but that will be a subject of the next article. Instead, the focus here will be to discuss accountabilities for potential privacy, security, and patient safety riskes that might arise from SMART on FHIR implementations.

Source system vendors will be accountable for conducting the security threat and risk assessment of their APIs to ensure traditional exploits like SQL injection or cross site scripting are locked down. But who is accountable for ensuring the SMART app doesn't store personal health information (PHI) or send it to another system?

For many people, this immediately conjures up images of nefarious developers providing SMART apps in order to access a gold mine of patient data. But there are many legitimate, government sanctioned needs for SMART apps. For example, an eReferral SMART app could be launched by a general practitioner using an EMR. The eReferral SMART app would query the EMR for provider and patient demographic data to auto populate sections in a referral form. The eReferral SMART app could then send the form data to a receiving system used by the specialist. The eReferral SMART app could even write data back to the EMR so that the general practitioner has a record of the referral. A similar use case was demonstrated at FHIR North 2018 with two different eReferral vendors and an HIS vendor. You can view the architecture and specification here: https://simplifier.net/guide/eReferraldraftiGuide/FHIRNorthCodeCamp

Let's presume the source system vendor is accountable for declaring which SMART apps work with its API, then who is accountable for authorizing specific users within an organization to launch SMART apps? Just because the source system can work with a SMART app, doesn't mean every instance of a source system has to allow everyone to use a SMART app.

Presumably the health information custodian (HIC) is responsible for identifying which users can launch which apps. If the HIC is a large academic teaching hospital, one could assume the IT department will work with various clinical groups and the chief privacy officer to identify which SMART apps can be launched.

But what about a 4-person primary care clinic? It's hard to imagine a situation where smaller community clinics have the resources and capability to assess SMART apps to determine which ones are appropriate to launch for users within the clinic.

Part of the assessment will include understanding what data the SMART app needs from the source system to help answer the question of which users should be allowed to launch the app. Should a physiotherapist be able to launch a SMART app that calculates breast cancer risk? Should the SMART app be allowed to write the risk score back to the HIS? While this might seem to open up a pandora's box of complexity, the answer is simple. Whatever permissions a user has in the source system should extend to the SMART apps they launch.

The previous examples also raise questions about accountability for potential patient safety risks. For example, who is accountable if a SMART app performs a calculation incorrectly and the results are used by a physician that leads to an adverse event for a patient? So long as the SMART app has the appropriate legal disclaimers then presumably accountability lies with the user, similar to the myriad risk calculator websites and mobile apps available today.

On the surface, SMART on FHIR implementations may seem to introduce new accountability paradigms for managing risks. However, upon closer examination it mirrors challenges that are well understood and already have frameworks in place for assessing and assigning accountability for risk.