DataArt SMART on FHIR Accelerator Information Blocking Use Cases

Case #1

A patient sees a primary care doctor. The patient's information is stored in the primary care physician's system. Assume that the physician refers the patient to a specialist, who has a separate practice in another location. The specialist will need access to all the patient information gathered by the primary care doctor. If the providers' information systems do not integrate with each other, the primary care physician is guilty of information blocking since their office cannot transfer medically necessary patient data.

The final rule introduced by ONC mandated that healthcare providers have information systems with FHIR APIs in place in order to receive certification, and in the near future part of the EHR certification process will include requirements around SMART on FHIR capabilities and FHIR APIs.

That creates an interesting situation because there is an EHR requirement that EHR vendors must fulfill in order to be certified and sell their product. On the other hand, healthcare providers become dependent on EHR vendors because it is healthcare providers who need to ensure they are not blocking information.

So, they should either push EHR vendors to speed up and introduce those capabilities into the EHRs they are already buying, or they should consider moving from the non-compliant EHR solution to one that does have SMART on FHIR. However, something needs to happen on both sides. EHR vendors need to make sure the FHIR APIs are there and healthcare providers need to make sure that the EHRs that they have do have those APIs.

Case #2

Speaking from the patient's perspective, it's one thing when two offices are talking to each other, but when a patient shares data, it is the patient's property. The healthcare provider takes responsibility for handling this data and making sure it is stored securely and remains private. The provider is also required to ensure that the patient has access to the data at all times.

Patient portals were one step toward ensuring access. But with the new final rule, data must be accessible on a machine-to-machine basis. Mobile device users spend time on a variety of applications. Those applications assume that there are APIs through which they can get access to relevant data.

Some of the apps, Apple Health for example, can potentially serve as aggregators of patient data. If you have multiple accounts within different EHRs at different providers, ideally what you want is to ensure that the accounts connected to this application can have data aggregated within the application, allowing the patient to use the data.

In order to get a comprehensive picture, you need more than a patient portal with a specific EHR. You need a tool that can gather all those data points, potentially from a few different systems, aggregate them, and present the data to the patient in a way that they can understand and act upon. The entire concept is based on the assumption that the party responsible for storing patient data will provide access to the patient, but through an API instead of a patient portal. It's not about the patient browsing the portal anymore – it's about another application that taps into the third party or healthcare provider's API on behalf of the patient.

According to the final rule, a patient portal is no longer sufficient. If you are not providing access through an API, you are not supporting data sharing or data access that is consumable by a computerized system. As such, you are guilty of information blocking. Both incentives and penalties are likely forthcoming.