Is my SMART on FHIR app ready for prime time? A review guideline for building and evaluating apps from proof of concept to production

Andrey Soares, PhD, Lisa M. Schilling, MD, MSPH
Data Science to Patient Value, University of Colorado School of Medicine, Aurora, CO

Abstract

Integrating third-party apps to EHRs is a concern to health system EHR IT leadership. The aim of this study is to identify guidelines from standards organizations and expert sources to review and approve SMART on FHIR apps to be developed and tested in a proof of concept/development environment and deployed to production. We identified and compiled a summary and checklist of technical and non-technical aspects for reviewing these apps.

Introduction

The proliferation of Electronic Health Record (EHR) Fast Healthcare Interoperability Resources (FHIR) use and (strong) platforms for mobile health integration such as Substitutable Medical Applications, Reusable Technologies (SMART) on FHIR have provided vast opportunities for leveraging data and bringing value to patients, health-care teams, payers, and health systems. The 21st Century Cures Act requires that a certified health information technology developer or entity have application programming interfaces (APIs) to allow interoperability and access to “all data elements of a patient’s electronic health record”. The dominant EHR industry method for meeting these requirements is via the use of FHIR to support data exchange, and SMART standards to support authorization and connection with the EHR. However, supporting 3rd party apps to exchange patient data with an EHR leads to a host of technical, regulatory, and privacy concerns for both health systems, who are responsible for securing their EHR systems and serving as guardians of patient data, and patients, who may not fully understand the consequences of data sharing.

Despite the straightforward development, authentication, and authorization of SMART on FHIR apps, there are other important factors to consider when developing apps or supporting their EHR integration. As EHR-integrated 3rd party apps run outside of EHR systems, they may need to comply with privacy and security regulations and be responsible for their accuracy, reliability, safety, and data security as well as risks and issues. An app collecting, storing and transmitting patient data outside of the EHR, for example, may require Health Insurance Portability and Accountability Act (HIPAA) compliance and provide and follow a privacy policy.

This study identified current guidelines and policies to address the collaborative needs of health system Information Technology (IT) leadership, researchers, and developers to mitigate technical concerns such as privacy, safety, and security of SMART on FHIR apps that interact with EHR systems. Health systems seeking to use EHR-integrated 3rd party app, either internally or as recommended apps for their patients, will want to review these apps using a vetted, systematic process. These guidelines should assist both app developers with pre-, post- and during-development review processes and the health system’s app review team with approvals and rejections of apps in a clear and consistent manner. For example, at Duke Health, new apps are vetted based on a standard process called the Service Transition Readiness Assessment (STRA), and Epic App Orchard has a submission questionnaire for vetting apps with questions related to their principles of qualities of ‘well-behaved’ apps.

Methods

We identified relevant guidelines for SMART on FHIR apps by searching for recommendations produced by standards organizations, such as Substitutable Medical Applications, Reusable Technologies (SMART), International Organization for Standardization (ISO), and the Open Web Application Security Project (OWASP), and 3rd party vendors sources, such as Epic Systems, Android Developers, and Apple Developers. To ensure that the guidelines are relevant and appropriate to the specific phase of app development, and not unnecessarily burdensome, we categorized them for application to three distinct stages: Proof of Concept (POC)/Development, Testing and Production, and we categorized each individual recommendation by the information source, recommendation type (policy or procedure), and category of concern addressed. From this we then synthesized the recommendations to create a single summarized checklist.

Results

Our preliminary results included the following categories of concern: safety, security, privacy, reliability, scalability, data integrity, system integrity, workflow, launch, performance, compatibility, stability, design and development,
updates, and legal responsibility, and over 150 individual recommendations or policies. Following the examples from Google Play, App Store and Epic App Orchard, we developed a review checklist to assist developers in obtaining approval for testing SMART on FHIR apps using a Proof of Concept/Development environment (e.g., FHIR server API endpoint with synthetic data and non-production instance of the EHR system) and a Test environment (e.g., FHIR server API endpoint with patient data and a production instance of the EHR), and for system leaders to evaluate and approve the apps.

**Discussion**

This study compiled a summary and checklist of technical and non-technical aspects for building and evaluating well designed, safe, secure and interoperable SMART on FHIR apps that intend to integrate with EHR systems to support patient care. The protection of patient data and privacy is of the utmost priority to health systems. Health systems and physicians that either recommend EHR-integrated apps to their patients or use internal apps to supplement their own EHR functionality need to have systematic and robust processes in place to ensure the privacy, security and safety of their own EHR and IT systems. Health system and hospitals need policies and concrete steps to evaluate the safety and performance consequences on their critical IT systems before integrating either vendor- or investigator-developed applications, whether for research or clinical care. For example, apps should be assessed and monitored as to the FHIR Resources used, how they store and potentially share patient information, how they communicate with other external apps and web services, and how they collect and store patient data on external repositories and databases. Having well developed and vetted review processes that align with the developmental stage of the app, from proof of concept to production, will facilitate collaboration and partnerships between health systems and health innovators, researchers and industry, and should contribute to the development and adoption of quality applications. This project is a work in progress and future directions include evaluating the selected guidelines with internally developed applications and seeking feedback about the quality of the recommendations from key stakeholders such as IT leaders and physicians.

**References**