SMART on FHIR with Okta

Leveraging Okta's platform for a key healthcare interoperability standard
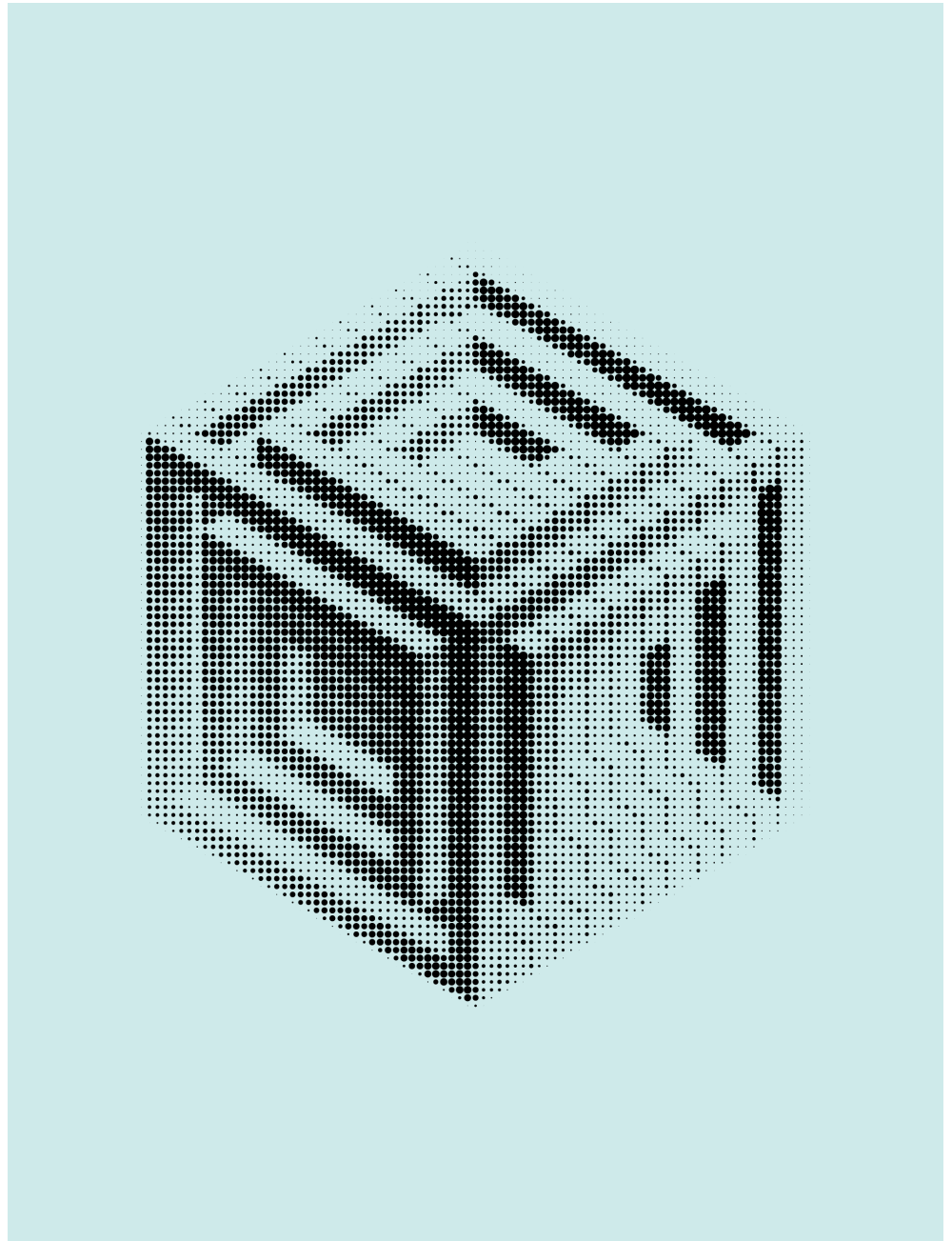
Okta Inc.

100 First Street

San Francisco, CA 94105

info@okta.com

1-888-722-7871

okta

Okta SMART on FHIR

What is the SMART on FHIR requirement, and why does it matter for healthcare insurance providers?

Today, there isn't an easy way to safely share patient data across the healthcare ecosystem, often leading to poor patient care and higher costs. In May of 2020, the U.S. Centers for Medicare & Medicaid Services (CMS) released the Interoperability and Patient Access final rule (CMS-9115-F), which aims to help solve this problem.

The Interoperability and Patient Access final rule identifies two baseline standards, Substitutable Medical Applications, Reusable Technologies (SMART) and FHIR® – Fast Healthcare Interoperability Resources to make interoperability easier and safer.

In order to comply with the Interoperability and Patient Access final rule, CMS-regulated payers, such as certain healthcare insurance providers, must provide a standardized Application Programming Interface (API) for patients to access their healthcare-related data following the FHIR standard. Applications that access a patient's health data may require patient consent/authorization and must follow the SMART standard.

Most off-the-shelf identity products are not fully capable of meeting the patient consent/authorization requirements on their own, and must be further enhanced to meet the interoperability needs set forth by CMS.

How can Okta help healthcare insurance providers comply with SMART on FHIR?

Reference implementation that extends Okta's authorization service as a platform to meet the interoperability needs set forth by CMS is available on GitHub.

Below is the logical flow to access patient information using Okta SMART on FHIR:

1. Patient accesses an app developed using the SMART & FHIR standards

2. To access patient information, the app will authenticate the patient using Okta including Multi-factor authentication (MFA) if desired

3. Okta will then redirect the patient to the consent/patient selection screen

4. Okta will issue the requested OAuth2 token after consent is given

5. Authorization proxy will enhance the token to meet the SMART authorization standard

6. App can then access patient information via FHIR API using the SMART authorization token
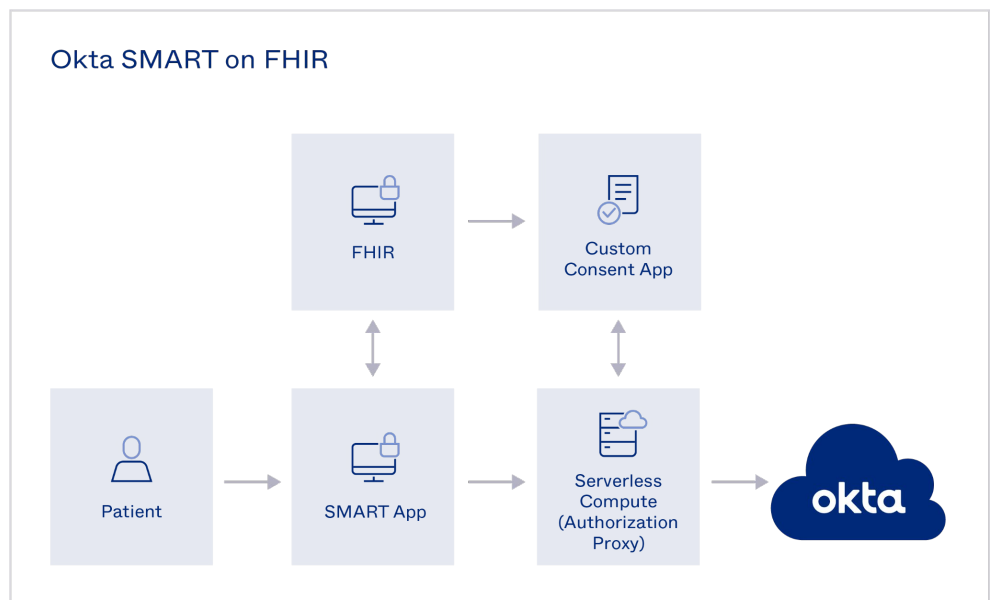
Okta SMART on FHIR

Benefits to Okta's SMART on FHIR Approach

Below is the logical flow to access patient information using Okta SMART on FHIR:

- Okta's secure, extensible and modern identity platform makes it easy to connect any user to any application, either with out-of-the-box integrations to apps like Cerner, Epic, and Workday or for custom solutions like patient or member portals including SMART on FHIR capabilities.

- Okta's Regulated Community Cloud meets some of the most rigorous compliance requirements, including HIPAA compliance and has also achieved a FedRAMP Moderate ATO. For more information about Okta and security, check out the Okta Security Technical Whitepaper

- Okta helps healthcare insurance providers' development teams increase agility by offloading the complexity of building an identity engine so developers focus on building the next innovative app

Additional Resources

Policies and Technology for Interoperability and Burden Reduction
Okta Security Technical Whitepaper
Okta for Healthcare

While this article discusses certain legal concepts, it does not constitute legal advice. It is provided for informational purposes only. For legal advice regarding your organization's compliance needs, please consult your organization's legal department. Okta makes no representations, warranties, or other assurances regarding the content of this article. Information regarding Okta's contractual assurances to its customers can be found at okta.com/agreements.