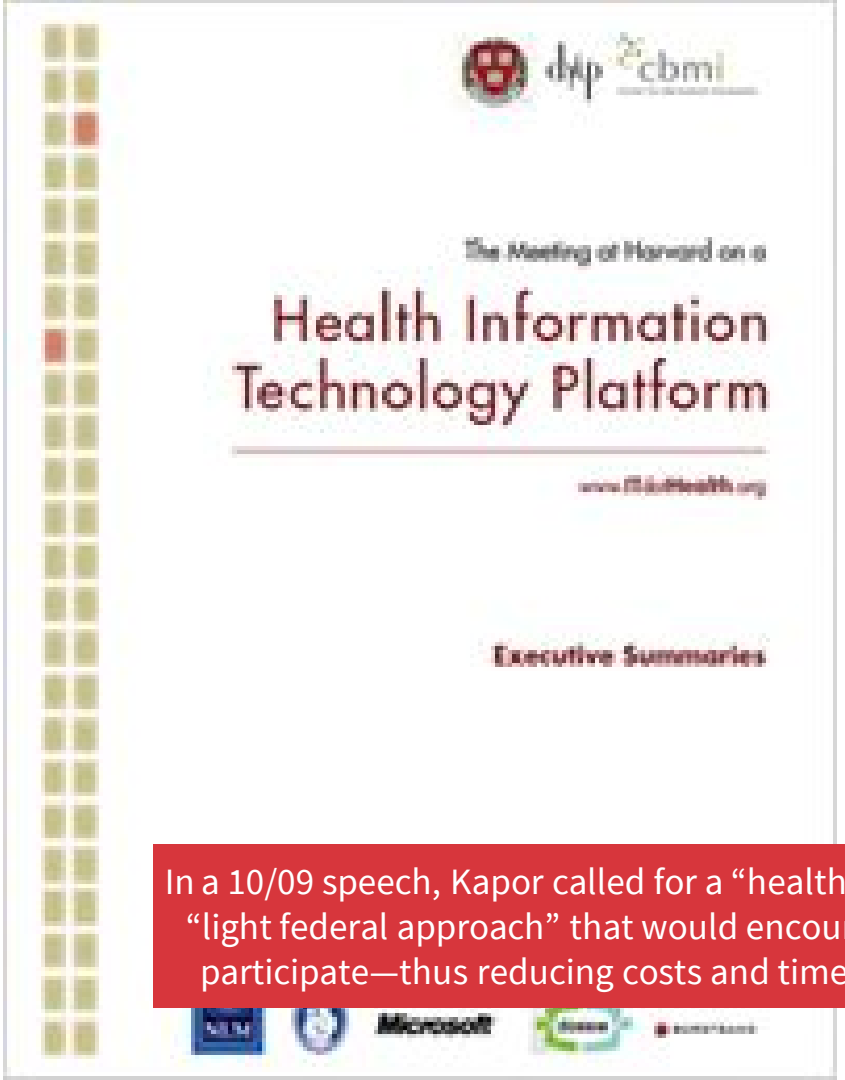
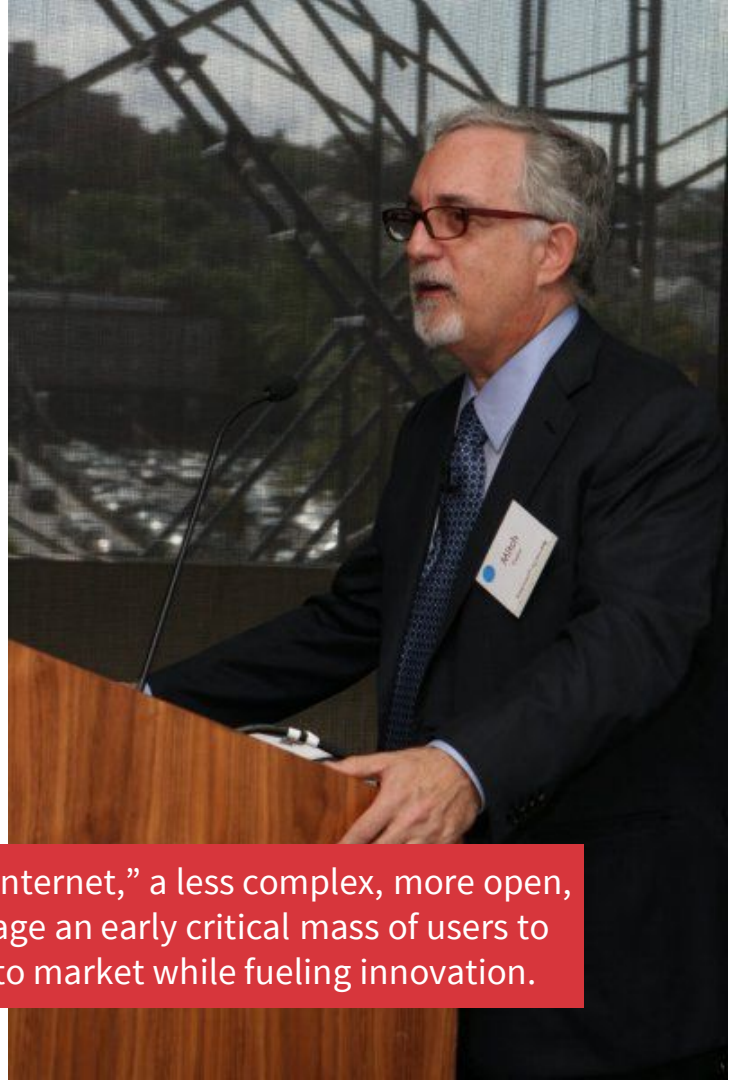
Health Internet ~
How the CMS Blue Button and FHIR APIs for EHR Data can Support Care Redesign

@aneeshchopra

www.navhealth.com





In a 10/09 speech, Kapor called for a “health Internet,” a less complex, more open, “light federal approach” that would encourage an early critical mass of users to participate—thus reducing costs and time to market while fueling innovation.

“All-in” Embrace of Open APIs for Data Exchange

Regulations, industry response aligned on technical capability

MU3: “Access to ONC-Certified API”

Certification Criteria (2015 Edition)

“The 2015 Edition includes **“application access”** criteria…to the **Common Clinical Data Set** via an **application programming interface** (API).**”**

HL7® FHIR®
ARGONAUT PROJECT

“The purpose…is to rapidly develop **a first-generation FHIR-based API** and Core Data Services specification…based on **Internet standards** and architectural patterns and styles.”

Voluntary, Industry Consensus Effort

February 2017

1. Consistent access to data (Common Clinical Data Set)
2. Consistent schema in returned data (Data Access Framework)
3. Open Implementation & Testing Framework (Sync for Science)

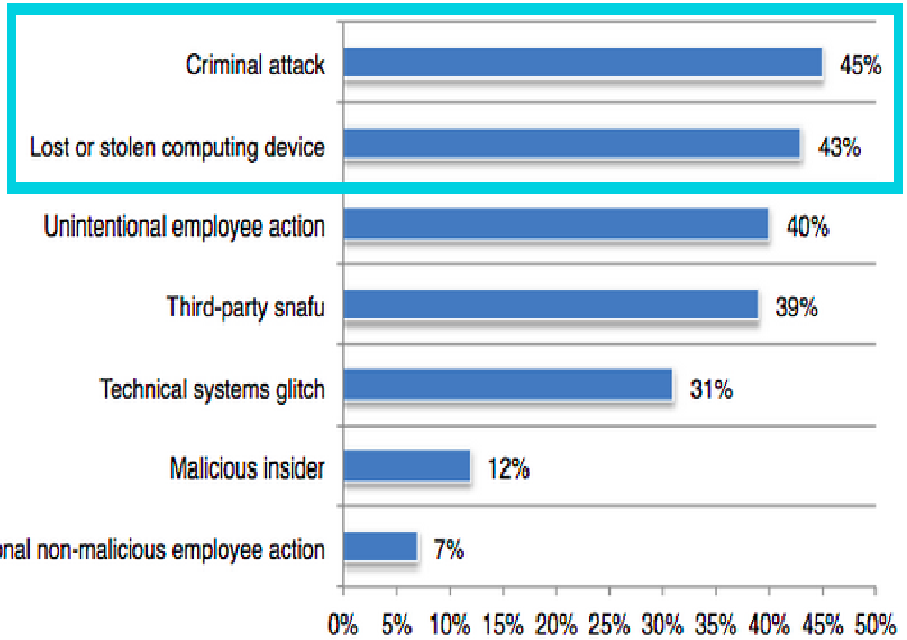
2017 Road Map includes support for scheduling, provider directory, and “CDS Hooks” (mechanism for integrating 3rd party decision support services to workflow)

Source: argonautproject.org; healthIT.gov; https://www.healthit.gov/policy-researchers-implementers/health-it-legislation-and-regulations; http://www.vita.virginia.gov/Library/default.aspx?id=6442474293

Opening Up While Locking Down

"API-First" approach adds security protection by monitoring use

What was the root cause of the healthcare organizations' data breach?
More than one response permitted



API vs. "Point to Point"

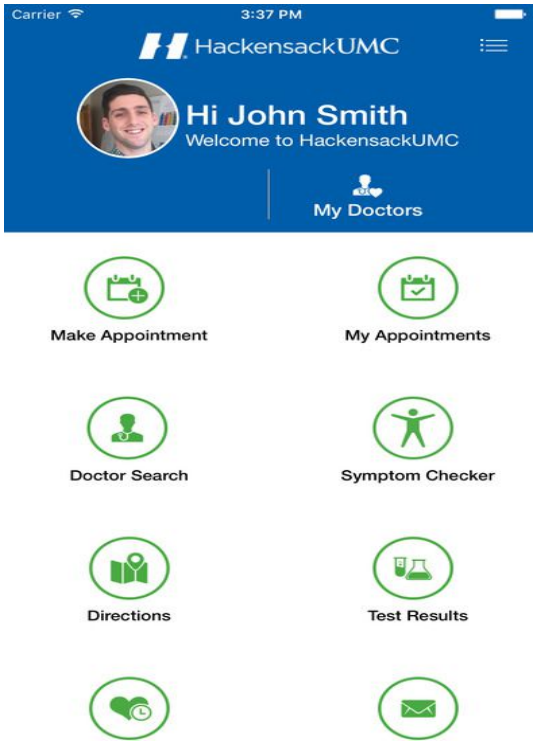
1. API-first approach to facilitate controlled access to data
2. Single point of "truth" for connected mobile, web apps
3. Real-time analytics to monitor use vs. shipping "blind" flat files

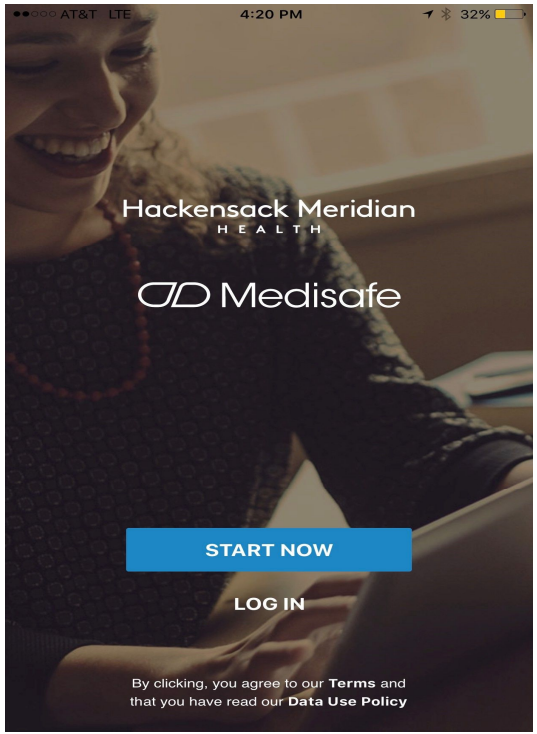
"Built-in" Security–APIs enforce a consistent protection mechanism across all channels with built-in authentication, authorization, and threat protection

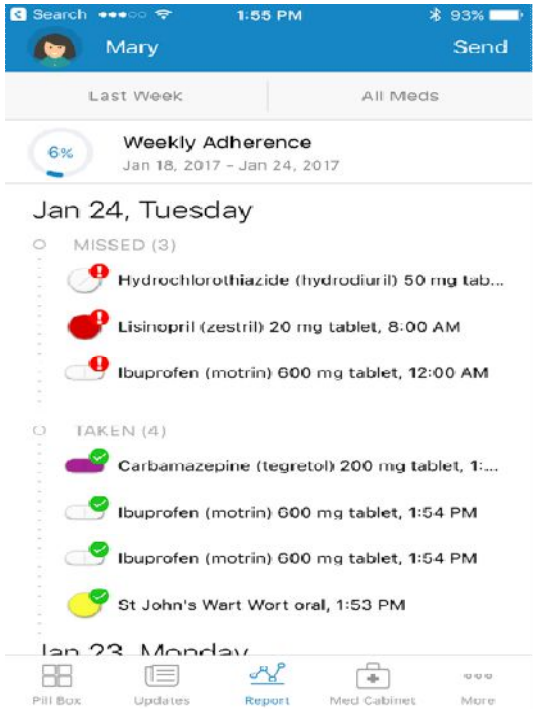
Source: The Ponemon Institute, "Fifth Annual Privacy and Security of Healthcare Data Report", May 2015

The “Connected Apps” Era

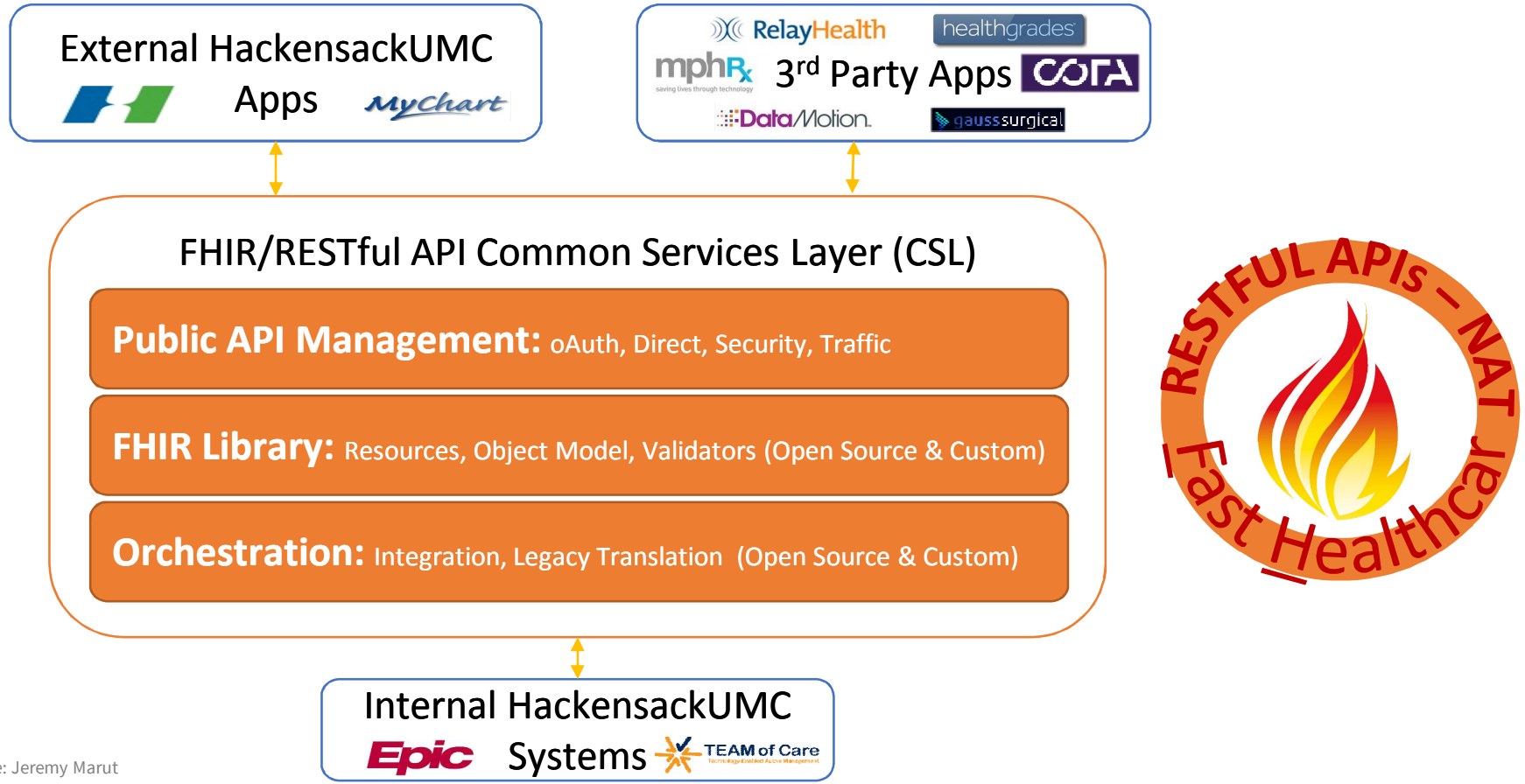
Hackensack Meridian Health opens up many digital paths for patients







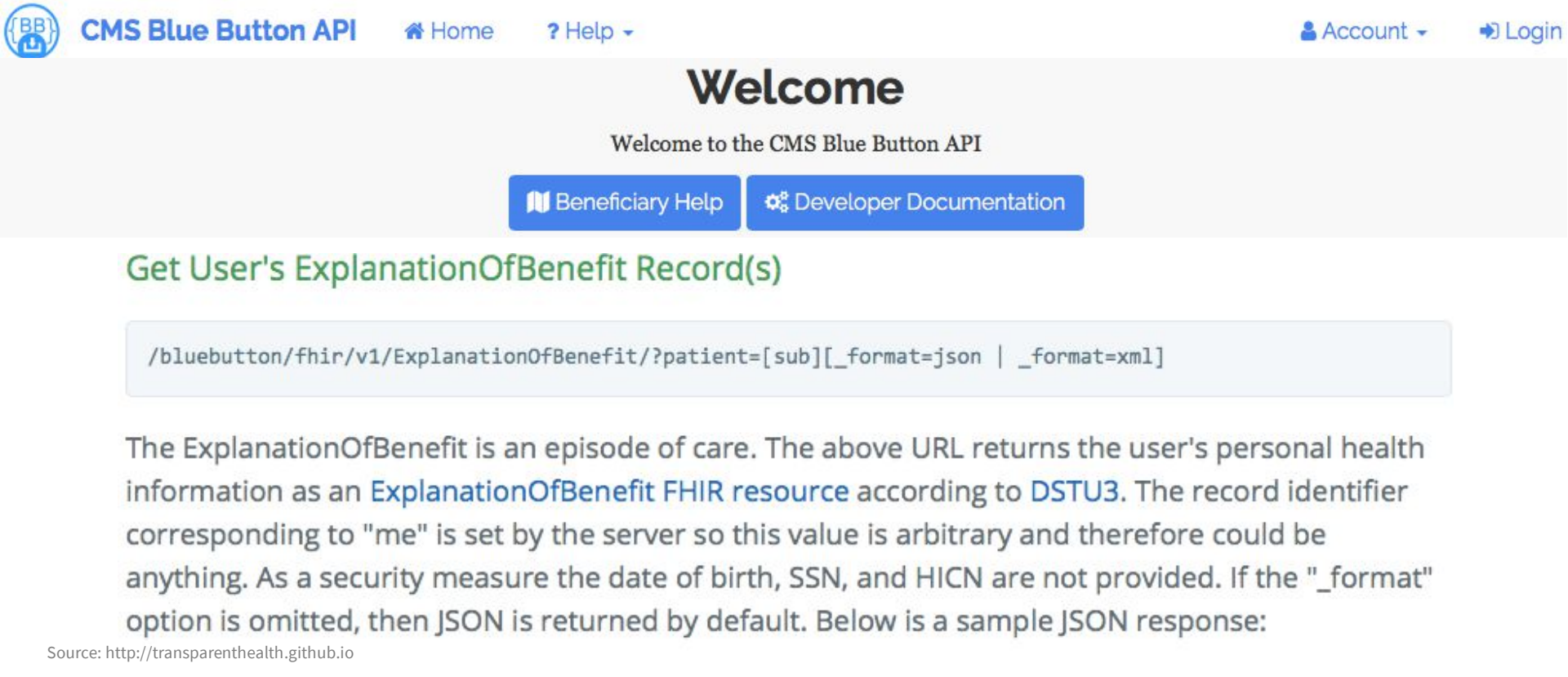
API-First Approach Flips Integration Upside Down



Source: Jeremy Marut

CMS “Blue Button” on FHIR (2017 Launch?)

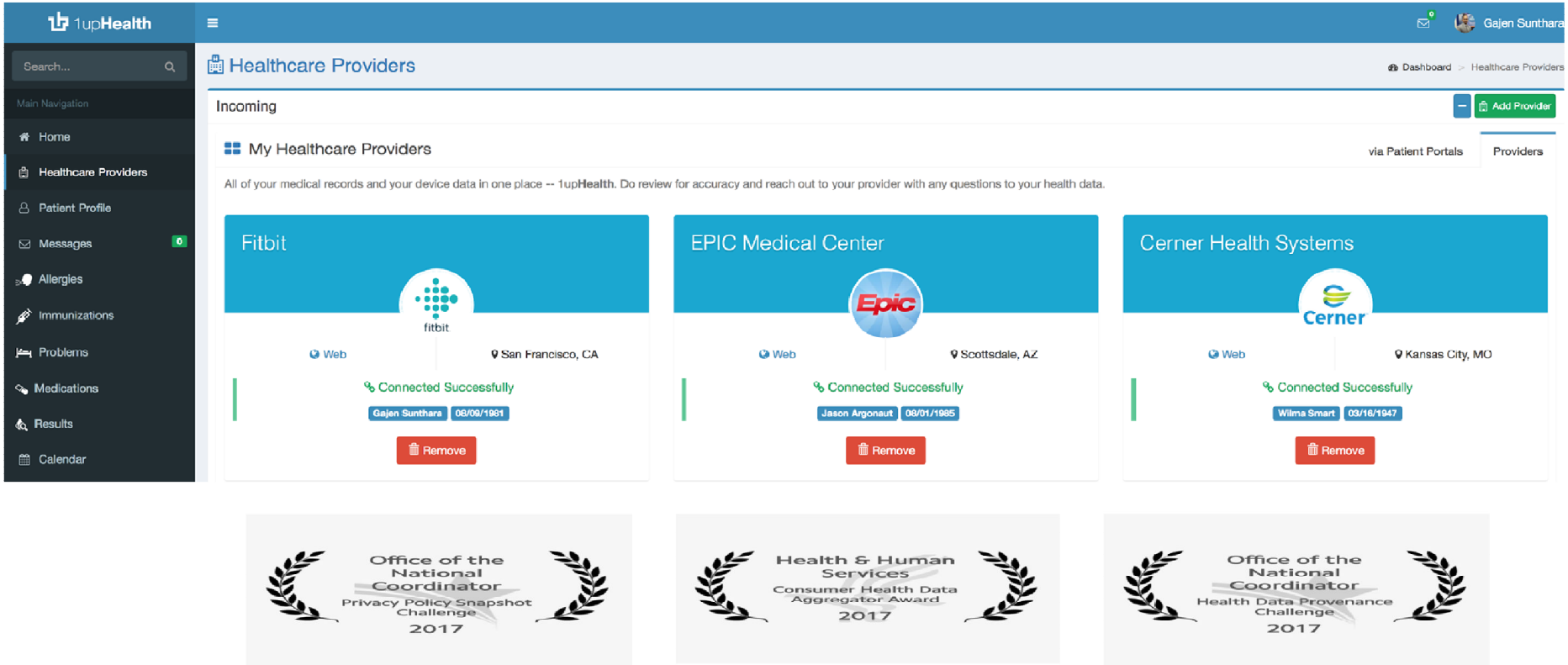
Application access to 2010 launch of consumer data access service



Source: http://transparenthealth.github.io

Interop via Consumer Directed Exchange

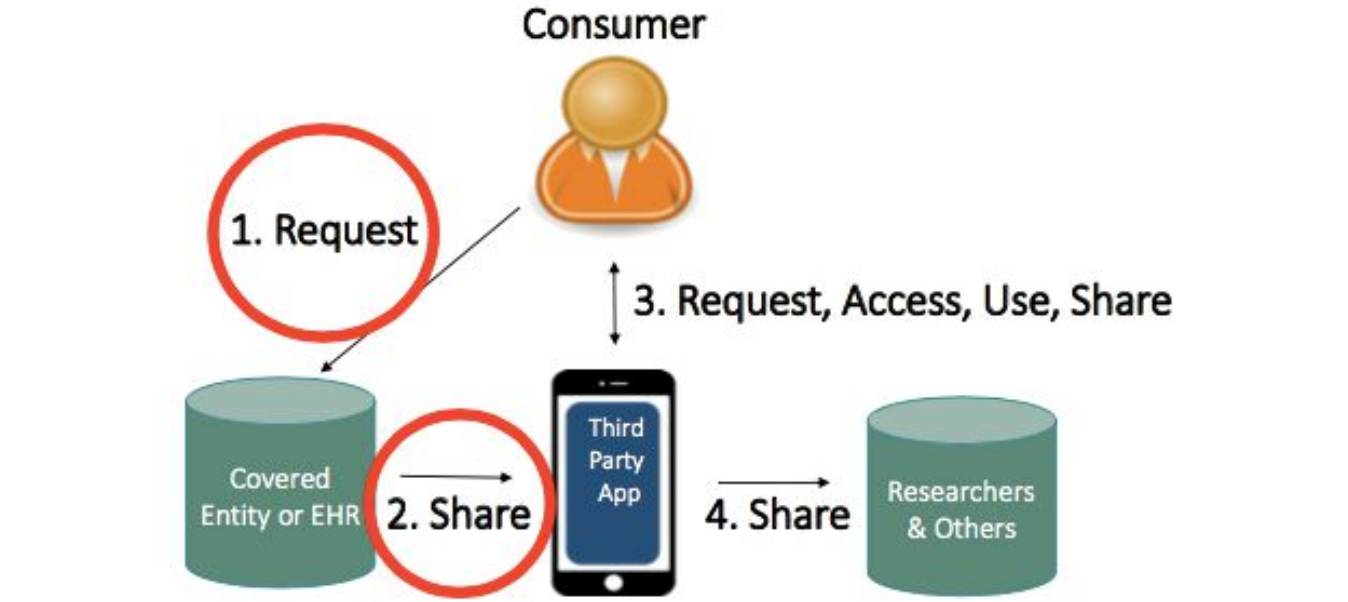
HHS prize competitions aims to demonstrate art of the possible



Source: 1uphealth.care

Multi-stakeholder Alliance to Accelerate Progress

CARIN Alliance launches to make consumer-directed exchange work



Eliminate the business and policy barriers associated with the implementation of the FHIR APIs

Source: carinalliance.com

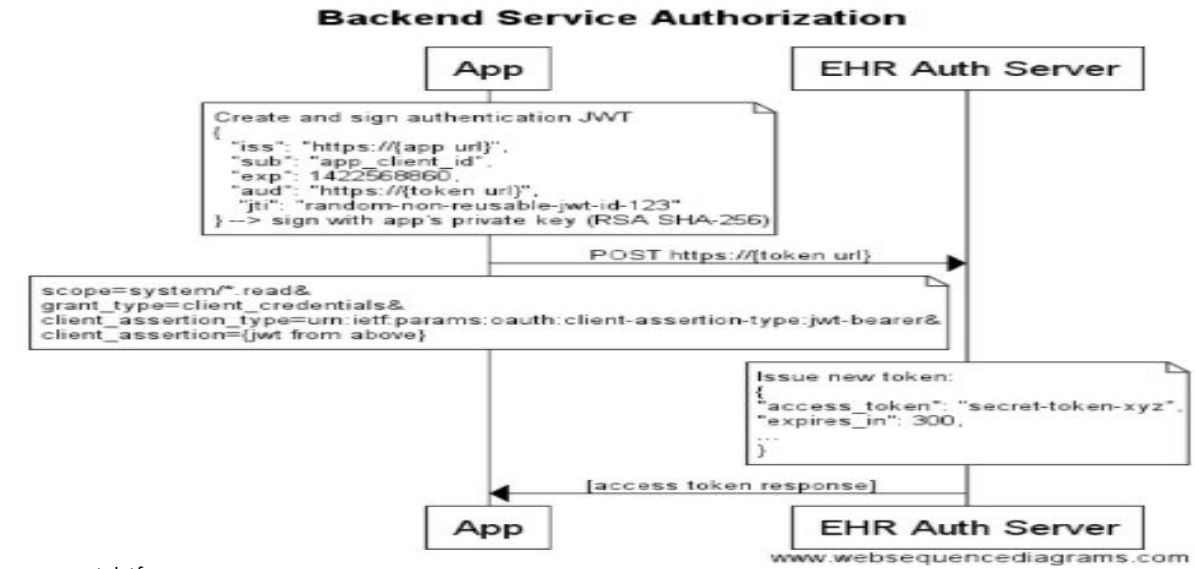
SMART “Backend Services” Draft Standards

Need “Coalition of the Willing” to test, iterate implementation guide

Obtaining an access token

By the time a backend service has been registered with the EHR, the key elements of organizational trust are already established. That is, the app is considered “pre-authorized” to access clinical data. Then, at runtime, the backend service must obtain an access token in order to work with clinical data. Such access tokens can be issued automatically, without need for human intervention, and they are short-lived, with a *recommended expiration time of fifteen minutes*.

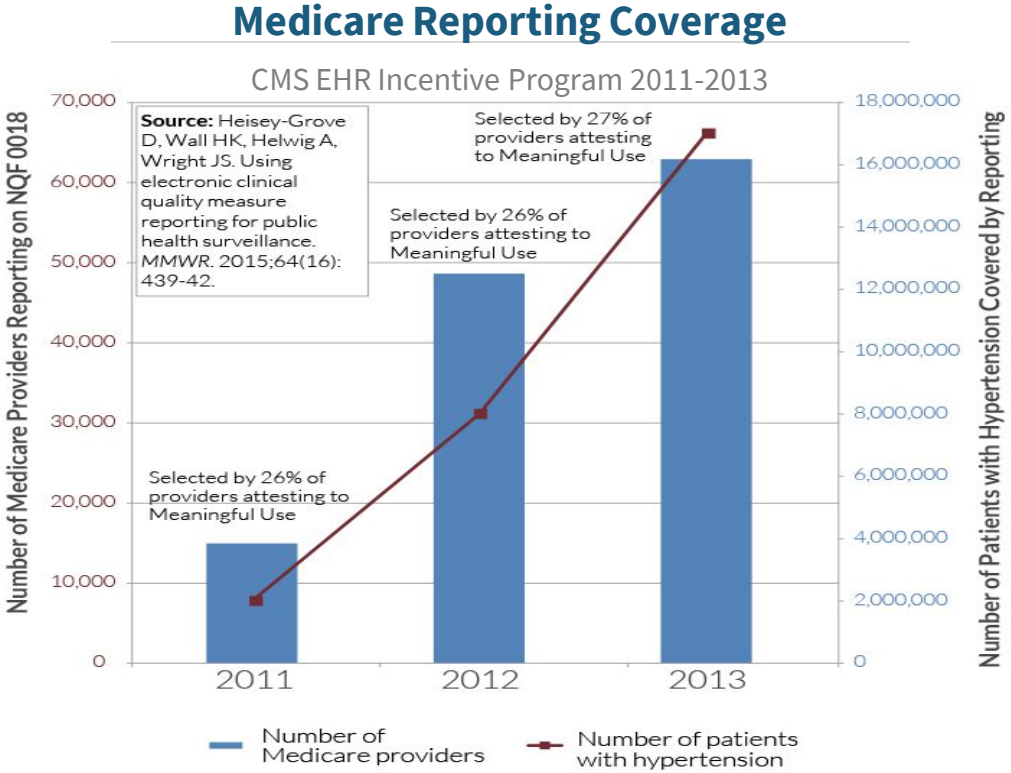
To obtain an access token, the service uses an OAuth 2.0 client credentials flow, with a JWT assertion as its client authenticaiton mechanism. The exchange, depicted below, allows the backend service to authenticate to the EHR and request a short-lived access token:

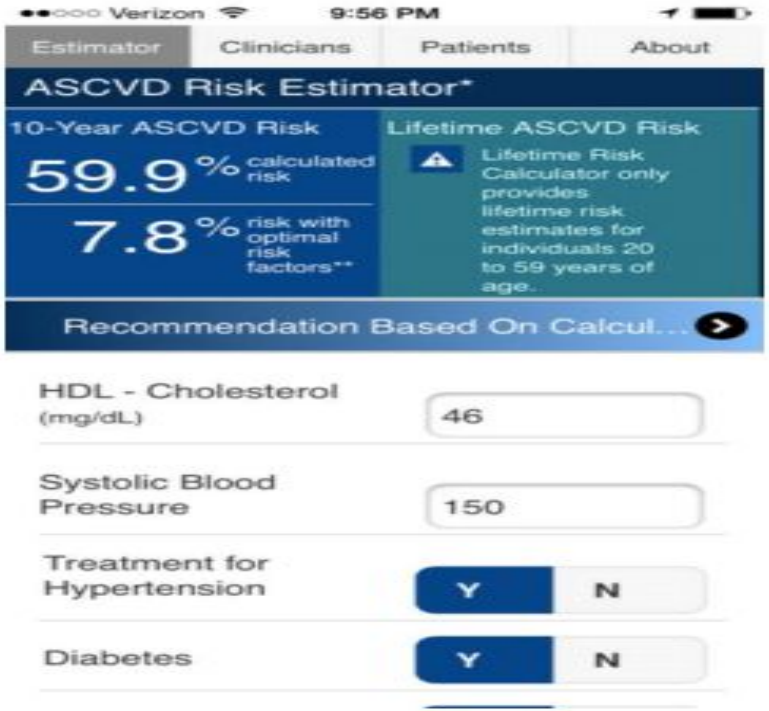


Source: smartplatforms.org

Connecting the Dots on Care Delivery Reform

"Million Hearts" campaign invokes open data, connected apps, pmt reform





Source: https://innovation.cms.gov/initiatives/Million-Hearts-CVDRRM/; https://millionhearts.hhs.gov/data-reports/data.htm;