TOMORROW, TODAY.

Cerner *code* Learning Lab 2017

Cerner®

Understanding OAuth

Background & Tutorial based on Sync for Science

Josh Mandel

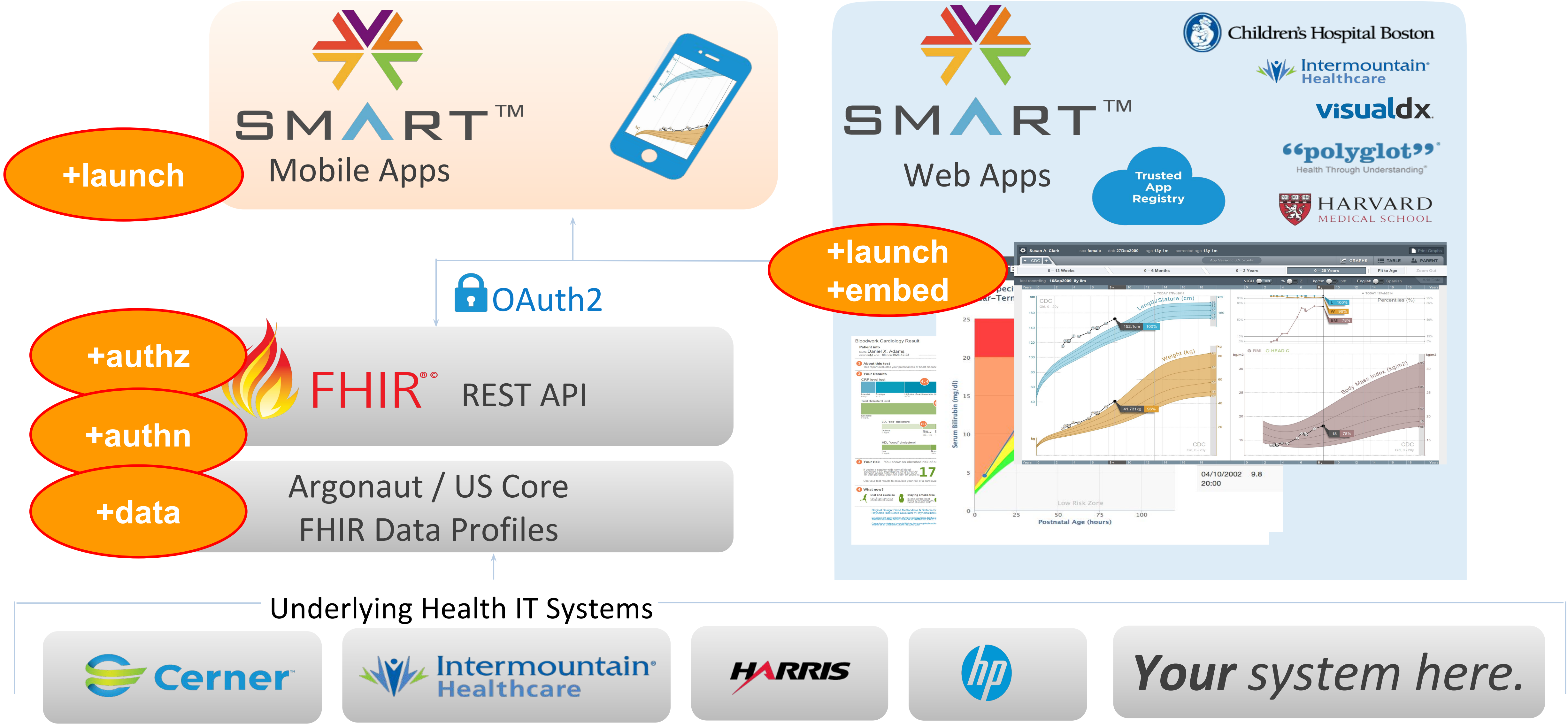
SMART Health IT Architect

10-Oct 2017

TOMORROW, TODAY.

Cerner *code* Learning Lab 2017

SMART on FHIR®© – Open Platform Architecture



SMART™

Mobile Apps

+launch

SMART™

Web Apps

Trusted App Registry

Children's Hospital Boston

Intermountain Healthcare

visualdx

"polyglot" Health Through Understanding

HARVARD MEDICAL SCHOOL

+launch
+embed

OAuth2

+authz

+authn

+data

FHIR®© REST API

Argonaut / US Core FHIR Data Profiles

Underlying Health IT Systems

Cerner

Intermountain Healthcare

HARRIS

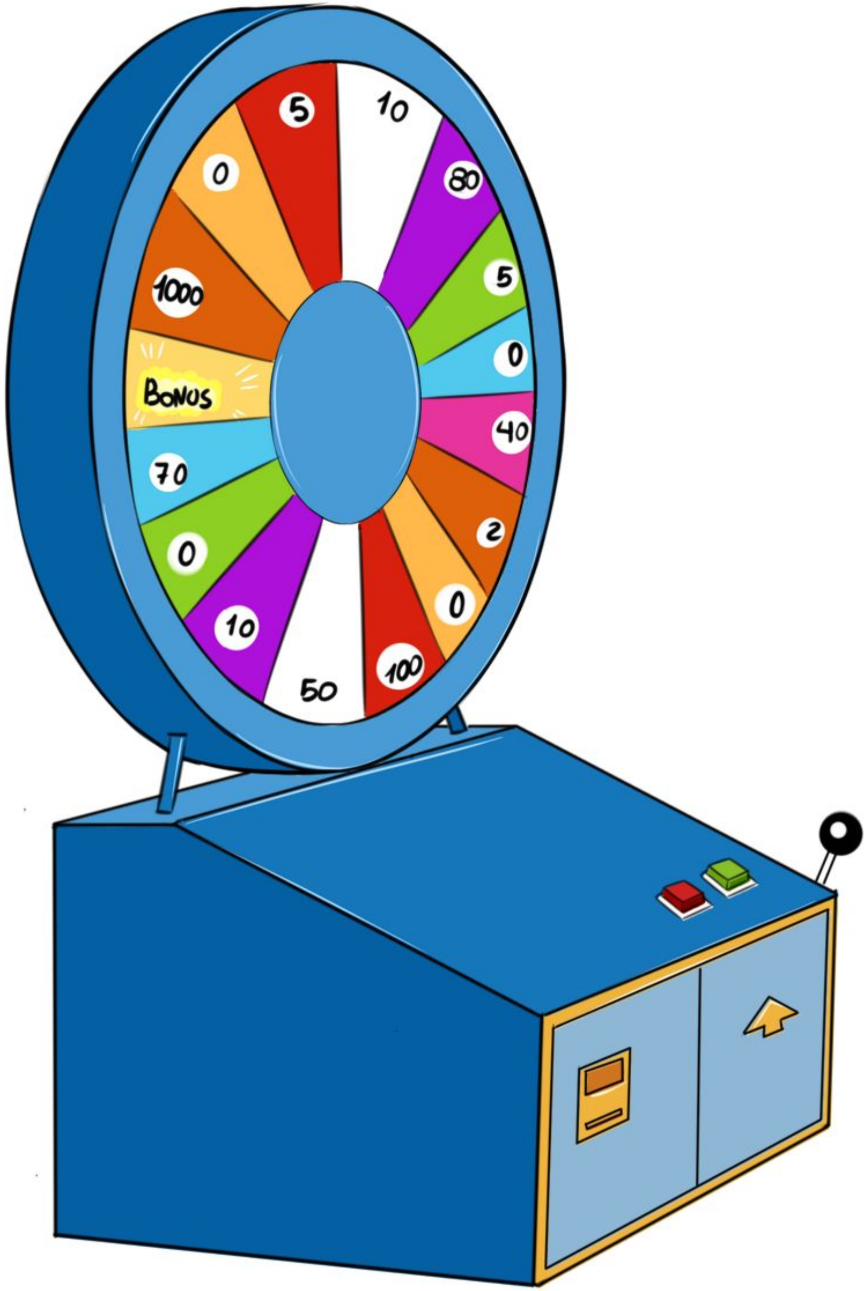
hp

Your system here.

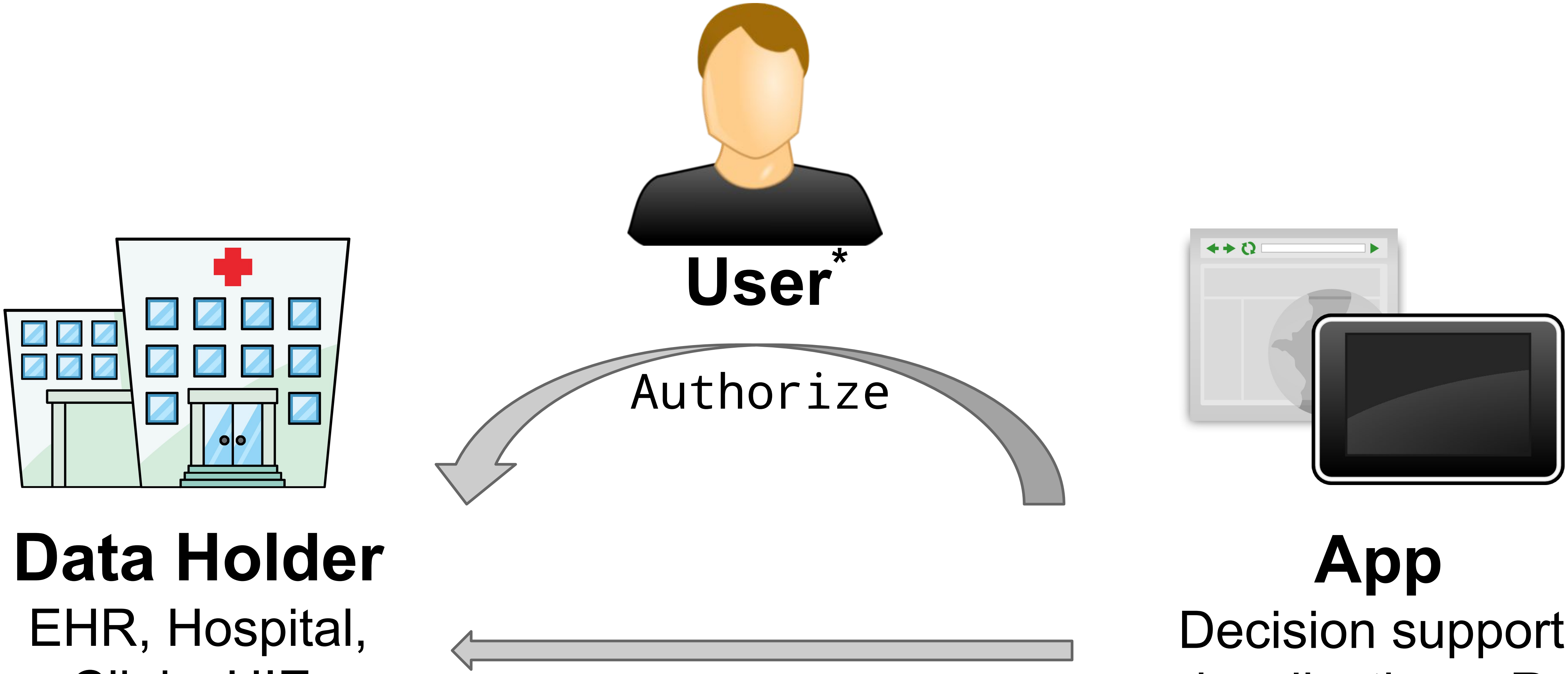
Use-Case-o-matic

Pick one from each row!

User	*clinician*, patient, none
Start from	*EHR*, portal, *none*
Access	*patient*, *population*
Duration	*brief*, long-term
Architecture	*confidential*, *public*



OAuth 2 shines at "access delegation"



User*

`Authorize`

Data Holder

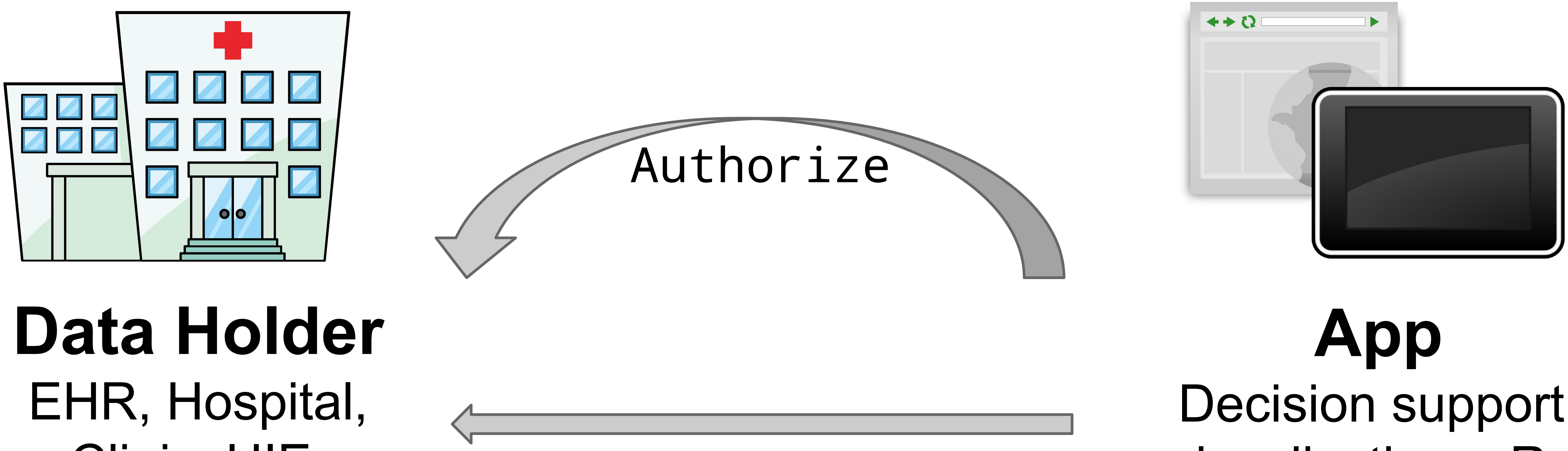
EHR, Hospital,
Clinic, HIE,
Lab, Insurer, etc.

```
GET /ehr/data
(etc.)
```

App

Decision support,
visualization, eRx,
pop health, etc.

OAuth 2 also supports "2-legged" auth



Authorize

`GET /ehr/data`
`(etc.)`

Data Holder

EHR, Hospital,
Clinic, HIE,
Lab, Insurer, etc.

App

Decision support,
visualization, eRx,
pop health, etc.

OAuth 2: Two examples!

Static HTML5 + JavaScript app (Easy to write, host...)

iOS app

[register with the EHR]

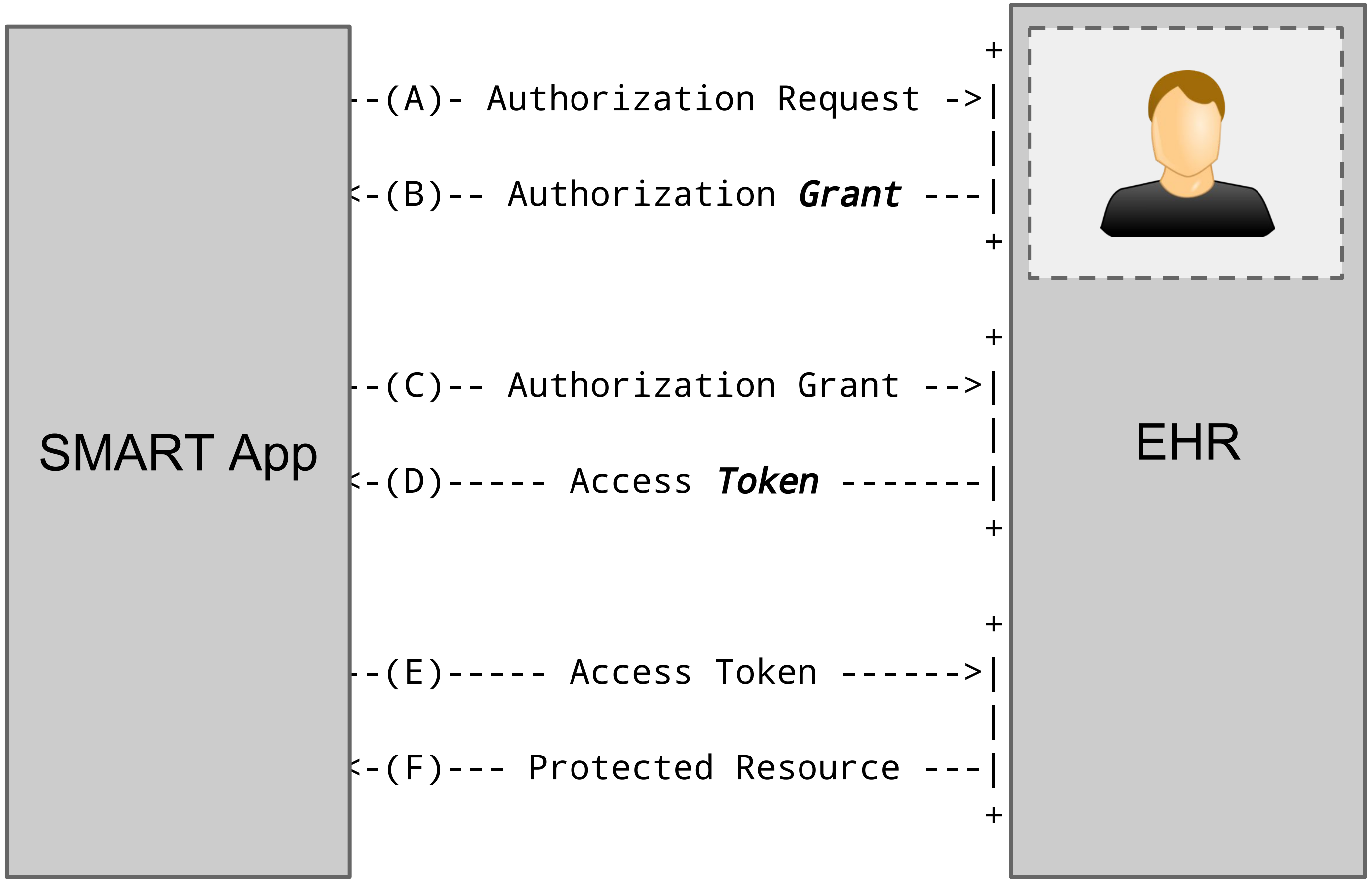
authorize to read *one patient's record*

get **access token**

access protected FHIR **resources**

OAuth 2: The abstract process

1.2. Protocol Flow



```
                               +
-(A)- Authorization Request ->|
                               |
<-(B)-- Authorization Grant ---|
                               +

                               +
-(C)-- Authorization Grant -->|
                               |
<-(D)----- Access Token -------|
                               +

                               +
-(E)----- Access Token ------>|
                               |
<-(F)--- Protected Resource ---|
                               +
```

Figure 1: Abstract Protocol Flow

[Register]

Authorize

Get token

Access resources

OAuth 2 is a "framework"   :-/

Yes, spec can be ***abstract***

But also provides new, helpful structures…

- Access ***scope*** (a live negotiation)
- **Public** *vs.* confidential clients (e.g. web vs native)
- Specialized ***flows*** (for different use cases)

Access scope (a live negotiation)

1. *Client asks for set (a) of scopes*
2. *Authorization granted with set (b) of scopes*

Note: **(a) and (b) can differ!**

Let's look at some *examples*…

facebook, google drive, salesforce

Lessons about *scopes*

Scopes are independent, not composable

e.g. `"read write documents"` is **three scopes, not one**

Granularity is **critical**

e.g. *read all my files*, or *contact all my friends* can be too broad

Scopes are often **implicit** based on user

e.g. `https://www.googleapis.com/auth/drive.readonly` in *my account vs. yours*

Patient-specific apps, small scopes

Cardiac Risk app can ask for:

```
patient/Patient.read
patient/Observation.read
```

More complex Diabetes Monograph app:

```
patient/*.read
```

An e-prescribing decision support tool:

```
patient/MedicationRequest.write
```

Population-level apps, broad scopes

*"**Three-legged**" use case*

duling app

`user/Appointment.read`

`user/`**`Appointment.write`**

*"**Two-legged**" use case*

rs incoming lab observations

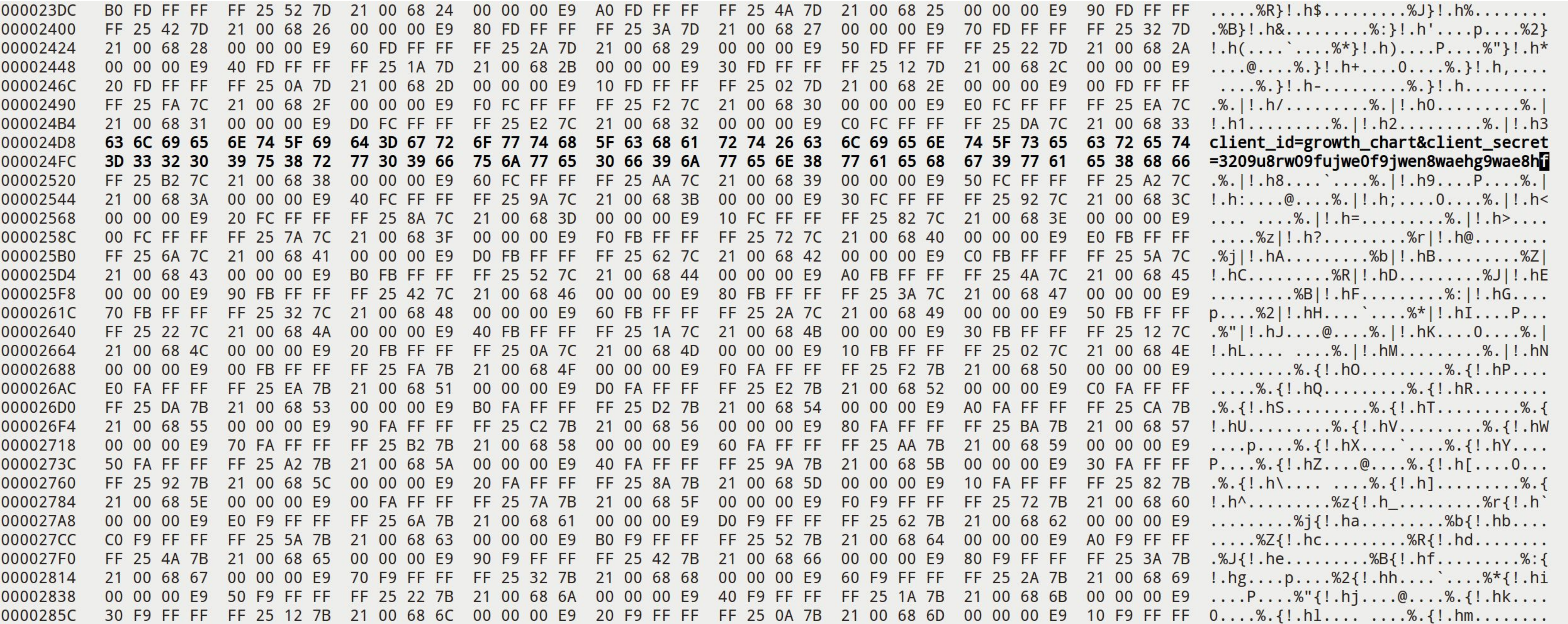
`system/Observation.read`

`system/`**`Alert.write`**

Question: population-level scopes limited by some principal?

- User? The app itself?
- (Allows separation of "done by" vs. "on behalf of"...)

Public *vs.* confidential clients



```
000023DC   B0 FD FF FF  FF 25 52 7D  21 00 68 24  00 00 00 E9  A0 FD FF FF  FF 25 4A 7D  21 00 68 25  00 00 00 E9  90 FD FF FF  .....%R}!.h$.........%J}!.h%........
00002400   FF 25 42 7D  21 00 68 26  00 00 00 E9  80 FD FF FF  FF 25 3A 7D  21 00 68 27  00 00 00 E9  70 FD FF FF  FF 25 32 7D  .%B}!.h&.........%:}!.h'....p....%2}
00002424   21 00 68 28  00 00 00 E9  60 FD FF FF  FF 25 2A 7D  21 00 68 29  00 00 00 E9  50 FD FF FF  FF 25 22 7D  21 00 68 2A  !.h(....`....%*}!.h)....P....%"}!.h*
00002448   00 00 00 E9  40 FD FF FF  FF 25 1A 7D  21 00 68 2B  00 00 00 E9  30 FD FF FF  FF 25 12 7D  21 00 68 2C  00 00 00 E9  ....@....%.}!.h+....0....%.}!.h,....
0000246C   20 FD FF FF  FF 25 0A 7D  21 00 68 2D  00 00 00 E9  10 FD FF FF  FF 25 02 7D  21 00 68 2E  00 00 00 E9  00 FD FF FF   ....%.}!.h-.........%.}!.h.........
00002490   FF 25 FA 7C  21 00 68 2F  00 00 00 E9  F0 FC FF FF  FF 25 F2 7C  21 00 68 30  00 00 00 E9  E0 FC FF FF  FF 25 EA 7C  .%.|!.h/.........%.|!.h0.........%.|
000024B4   21 00 68 31  00 00 00 E9  D0 FC FF FF  FF 25 E2 7C  21 00 68 32  00 00 00 E9  C0 FC FF FF  FF 25 DA 7C  21 00 68 33  !.h1.........%.|!.h2.........%.|!.h3
000024D8   63 6C 69 65  6E 74 5F 69  64 3D 67 72  6F 77 74 68  5F 63 68 61  72 74 26 63  6C 69 65 6E  74 5F 73 65  63 72 65 74  client_id=growth_chart&client_secret
000024FC   3D 33 32 30  39 75 38 72  77 30 39 66  75 6A 77 65  30 66 39 6A  77 65 6E 38  77 61 65 68  67 39 77 61  65 38 68 66  =3209u8rw09fujwe0f9jwen8waehg9wae8hf
00002520   FF 25 B2 7C  21 00 68 38  00 00 00 E9  60 FC FF FF  FF 25 AA 7C  21 00 68 39  00 00 00 E9  50 FC FF FF  FF 25 A2 7C  .%.|!.h8....`....%.|!.h9....P....%.|
00002544   21 00 68 3A  00 00 00 E9  40 FC FF FF  FF 25 9A 7C  21 00 68 3B  00 00 00 E9  30 FC FF FF  FF 25 92 7C  21 00 68 3C  !.h:....@....%.|!.h;....0....%.|!.h<
00002568   00 00 00 E9  20 FC FF FF  FF 25 8A 7C  21 00 68 3D  00 00 00 E9  10 FC FF FF  FF 25 82 7C  21 00 68 3E  00 00 00 E9  .... ....%.|!.h=.........%.|!.h>....
0000258C   00 FC FF FF  FF 25 7A 7C  21 00 68 3F  00 00 00 E9  F0 FB FF FF  FF 25 72 7C  21 00 68 40  00 00 00 E9  E0 FB FF FF  .....%z|!.h?.........%r|!.h@........
000025B0   FF 25 6A 7C  21 00 68 41  00 00 00 E9  D0 FB FF FF  FF 25 62 7C  21 00 68 42  00 00 00 E9  C0 FB FF FF  FF 25 5A 7C  .%j|!.hA.........%b|!.hB.........%Z|
000025D4   21 00 68 43  00 00 00 E9  B0 FB FF FF  FF 25 52 7C  21 00 68 44  00 00 00 E9  A0 FB FF FF  FF 25 4A 7C  21 00 68 45  !.hC.........%R|!.hD.........%J|!.hE
000025F8   00 00 00 E9  90 FB FF FF  FF 25 42 7C  21 00 68 46  00 00 00 E9  80 FB FF FF  FF 25 3A 7C  21 00 68 47  00 00 00 E9  .........%B|!.hF.........%:|!.hG....
0000261C   70 FB FF FF  FF 25 32 7C  21 00 68 48  00 00 00 E9  60 FB FF FF  FF 25 2A 7C  21 00 68 49  00 00 00 E9  50 FB FF FF  p....%2|!.hH....`....%*|!.hI....P...
00002640   FF 25 22 7C  21 00 68 4A  00 00 00 E9  40 FB FF FF  FF 25 1A 7C  21 00 68 4B  00 00 00 E9  30 FB FF FF  FF 25 12 7C  .%"|!.hJ....@....%.|!.hK....0....%.|
00002664   21 00 68 4C  00 00 00 E9  20 FB FF FF  FF 25 0A 7C  21 00 68 4D  00 00 00 E9  10 FB FF FF  FF 25 02 7C  21 00 68 4E  !.hL.... ....%.|!.hM.........%.|!.hN
00002688   00 00 00 E9  00 FB FF FF  FF 25 FA 7B  21 00 68 4F  00 00 00 E9  F0 FA FF FF  FF 25 F2 7B  21 00 68 50  00 00 00 E9  .........%.{!.hO.........%.{!.hP....
000026AC   E0 FA FF FF  FF 25 EA 7B  21 00 68 51  00 00 00 E9  D0 FA FF FF  FF 25 E2 7B  21 00 68 52  00 00 00 E9  C0 FA FF FF  .....%.{!.hQ.........%.{!.hR........
000026D0   FF 25 DA 7B  21 00 68 53  00 00 00 E9  B0 FA FF FF  FF 25 D2 7B  21 00 68 54  00 00 00 E9  A0 FA FF FF  FF 25 CA 7B  .%.{!.hS.........%.{!.hT.........%.{
000026F4   21 00 68 55  00 00 00 E9  90 FA FF FF  FF 25 C2 7B  21 00 68 56  00 00 00 E9  80 FA FF FF  FF 25 BA 7B  21 00 68 57  !.hU.........%.{!.hV.........%.{!.hW
00002718   00 00 00 E9  70 FA FF FF  FF 25 B2 7B  21 00 68 58  00 00 00 E9  60 FA FF FF  FF 25 AA 7B  21 00 68 59  00 00 00 E9  ....p....%.{!.hX....`....%.{!.hY....
0000273C   50 FA FF FF  FF 25 A2 7B  21 00 68 5A  00 00 00 E9  40 FA FF FF  FF 25 9A 7B  21 00 68 5B  00 00 00 E9  30 FA FF FF  P....%.{!.hZ....@....%.{!.h[....0...
00002760   FF 25 92 7B  21 00 68 5C  00 00 00 E9  20 FA FF FF  FF 25 8A 7B  21 00 68 5D  00 00 00 E9  10 FA FF FF  FF 25 82 7B  .%.{!.h\.... ....%.{!.h].........%.{
00002784   21 00 68 5E  00 00 00 E9  00 FA FF FF  FF 25 7A 7B  21 00 68 5F  00 00 00 E9  F0 F9 FF FF  FF 25 72 7B  21 00 68 60  !.h^.........%z{!.h_.........%r{!.h`
000027A8   00 00 00 E9  E0 F9 FF FF  FF 25 6A 7B  21 00 68 61  00 00 00 E9  D0 F9 FF FF  FF 25 62 7B  21 00 68 62  00 00 00 E9  .........%j{!.ha.........%b{!.hb....
000027CC   C0 F9 FF FF  FF 25 5A 7B  21 00 68 63  00 00 00 E9  B0 F9 FF FF  FF 25 52 7B  21 00 68 64  00 00 00 E9  A0 F9 FF FF  .....%Z{!.hc.........%R{!.hd........
000027F0   FF 25 4A 7B  21 00 68 65  00 00 00 E9  90 F9 FF FF  FF 25 42 7B  21 00 68 66  00 00 00 E9  80 F9 FF FF  FF 25 3A 7B  .%J{!.he.........%B{!.hf.........%:{
00002814   21 00 68 67  00 00 00 E9  70 F9 FF FF  FF 25 32 7B  21 00 68 68  00 00 00 E9  60 F9 FF FF  FF 25 2A 7B  21 00 68 69  !.hg....p....%2{!.hh....`....%*{!.hi
00002838   00 00 00 E9  50 F9 FF FF  FF 25 22 7B  21 00 68 6A  00 00 00 E9  40 F9 FF FF  FF 25 1A 7B  21 00 68 6B  00 00 00 E9  ....P....%"{!.hj....@....%.{!.hk....
0000285C   30 F9 FF FF  FF 25 12 7B  21 00 68 6C  00 00 00 E9  20 F9 FF FF  FF 25 0A 7B  21 00 68 6D  00 00 00 E9  10 F9 FF FF  0....%.{!.hl.... ....%.{!.hm........
```

Public *vs.* confidential clients

OAuth 2 explicitly classifies clients by:

Can you guard a `client_secret`*?*

→ **Different security considerations** apply.

Public client

Send user to

```
http://ehr/authorize?
  client_id=123&
  redirect_uri=https://hack.me
```

Anyone can construct this URL, *and get token* without (or with unprotected) `client_secret`
→ **Dangerous Practice**

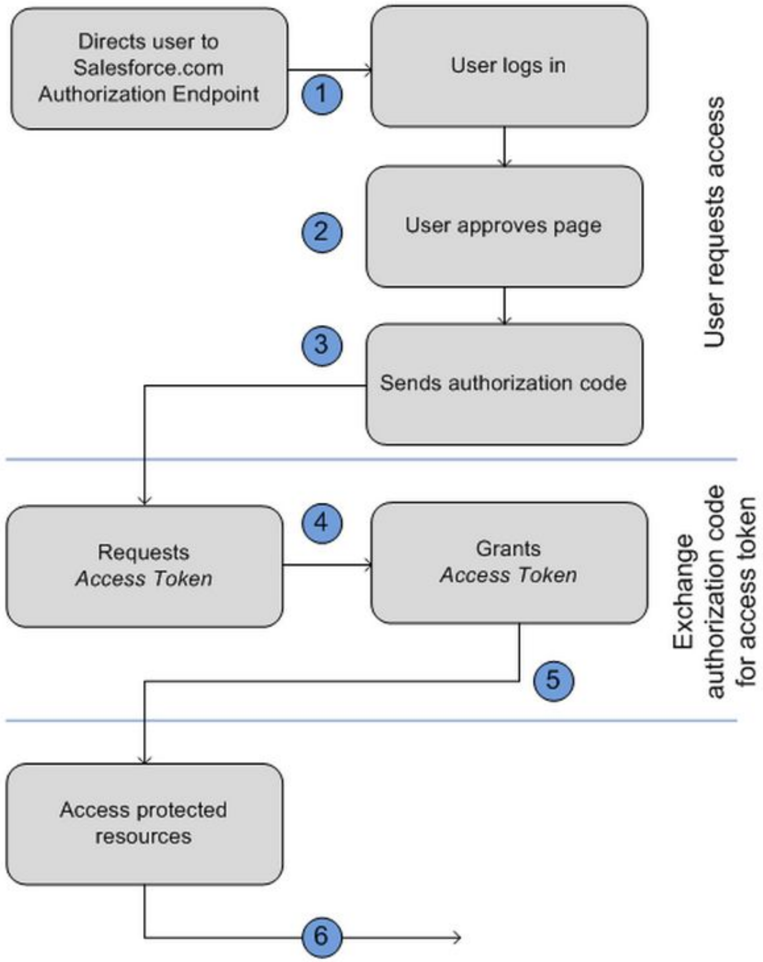
Specialized grant flows (three-legged)

Authorization Code

For **confidential** and **public** clients

Two steps:

1. authorize → code
2. exchange code → token



Specialized grant flows (two legged)

Client Credentials

- When a client is acting "on its own behalf"
- Trades `client_secret` for a scoped access token
- Better than protecting resources with `client_secret`!
- Similar to 2-legged OA1 PLAINTEXT

NB: other grants exist in OA2 core + extensions

Security Principle:

User-facing apps (web, mobile, etc.) *should use 3-legged OAuth + redirects*

***Not* two-legged auth**

EHR can ensure user is signed in

Access tokens map reliably to users

***Not* three-legged with client password grant**

2-factor auth, different sign-in requirements

Entering Authorization flow from EHR

Starting from an EHR session

URL-based context-passing

General launch parameters

```
[launch-url]?
  iss=https://fhir-api.smartplatforms.org&
  launch=some-opaque-context-id
```

Then app trades some-context-id for full launch context.

Entering Authorization flow from app

Key idea: re-use the machinery above.

1. *App redirects to EHR's "authorize" URL*
2. *App declares required context*

    e.g. "launch/patient launch/encounter"

3. *EHR "gathers" context as needed*

    e.g. user picks patient if needed

4. *EHR redirects to app's launch URL*

Adding on User Authentication

For example, via OIDC

```
{
   "sub": "248289761001",
   "profile": "Practitioner/123"
}
```

OIDC claim → FHIR Resource

```
"fhir_resource": "/Practitioner/456"
```

Allows signed token (JWT) with details like

- NPI
- Specialty
- Clinical Role

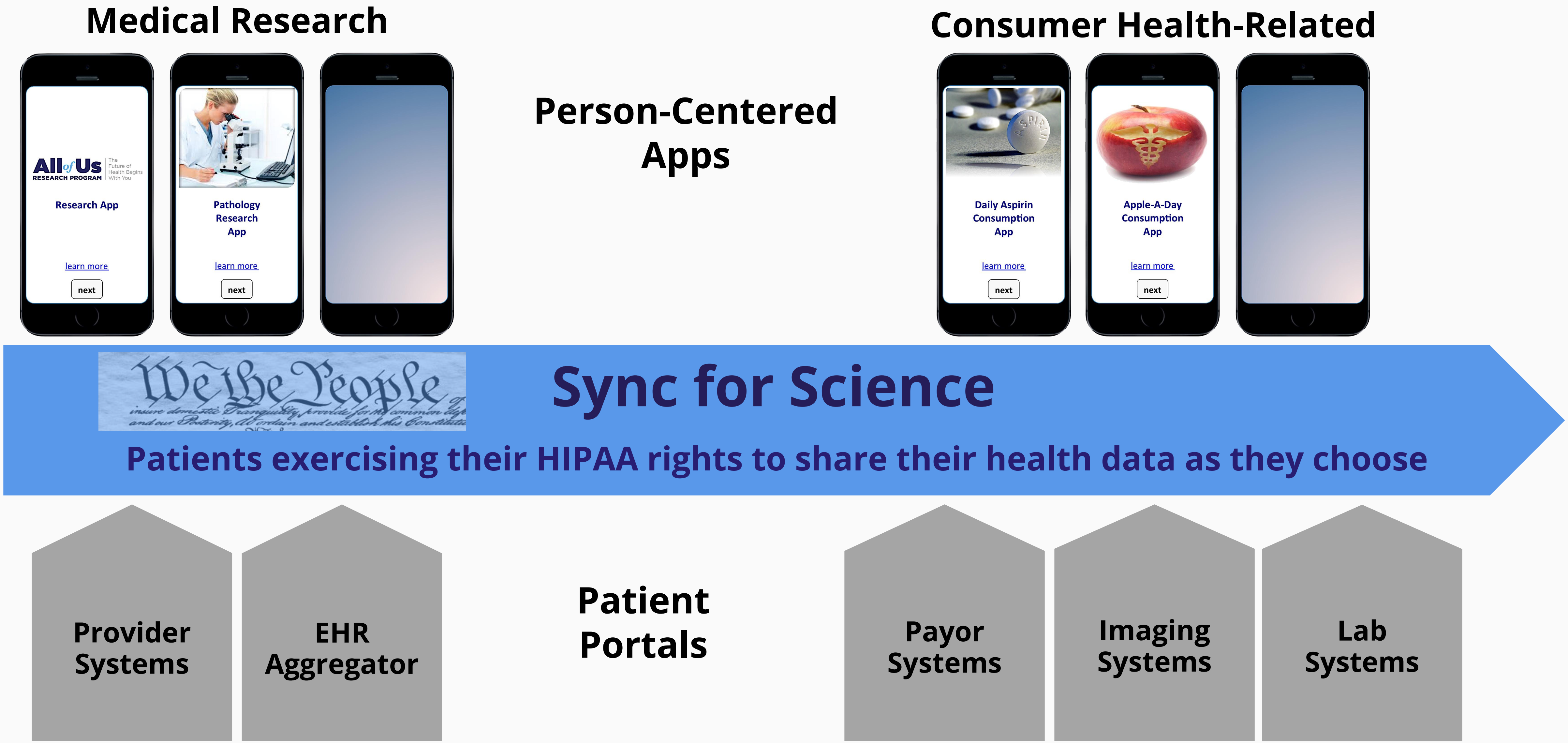
Questions

Demo

&

Discussion

S4S Platform – Supporting research, but not just research


All of Us RESEARCH PROGRAM
The Future of Health Begins With You
Research App
learn more
next
Pathology Research App
learn more
next
Daily Aspirin Consumption App
learn more
next
Apple-A-Day Consumption App
learn more
next
We the People
insure domestic Tranquility, provide for the common def
and our Posterity, do ordain and establish this Constitutio

Medical Research

Person-Centered Apps

Consumer Health-Related

Sync for Science

Patients exercising their HIPAA rights to share their health data as they choose

Provider Systems

EHR Aggregator

Patient Portals

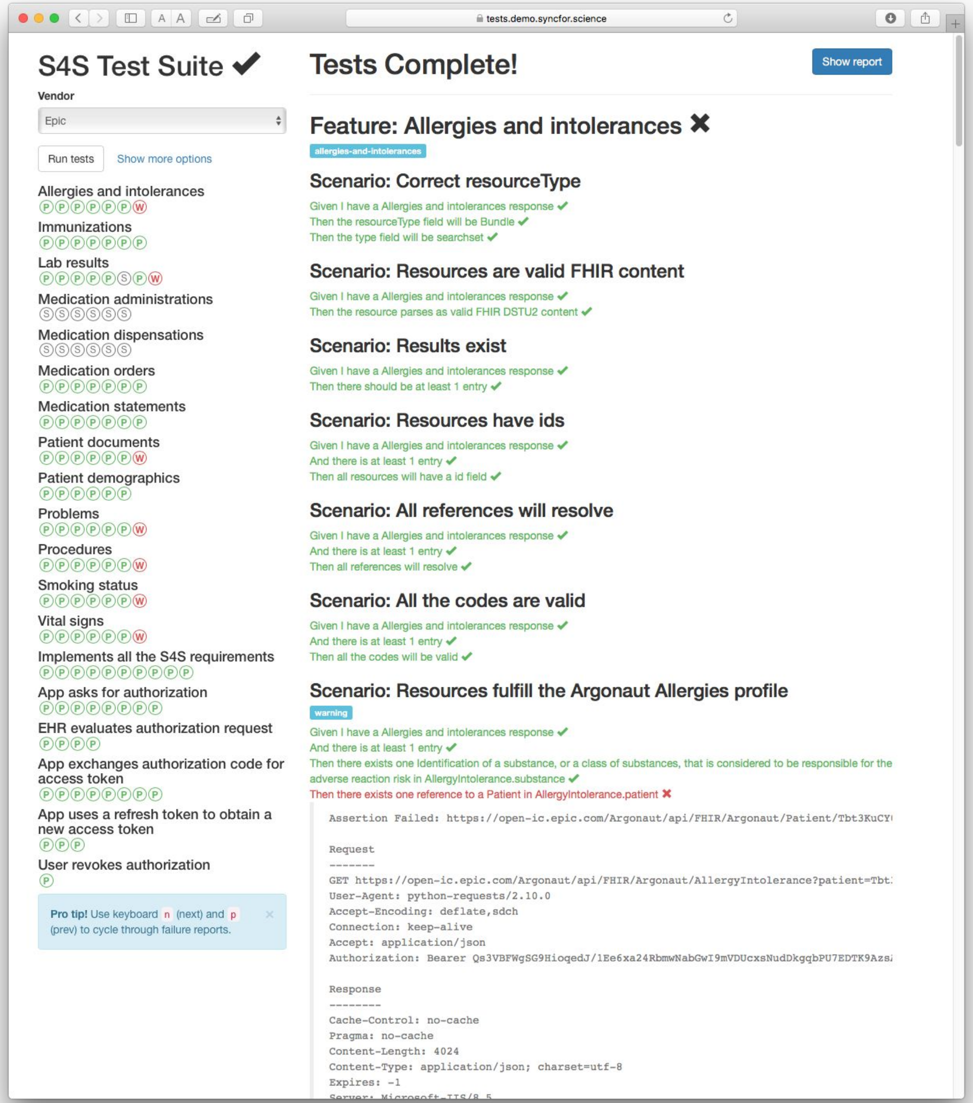
Payor Systems

Imaging Systems

Lab Systems

S4S Test Suite – Verifying EHR Compliance with S4S

SYNC FOR SCIENCE



S4S Test Suite ✓

Vendor: Epic

Allergies and intolerances
Ⓟ Ⓟ Ⓟ Ⓟ Ⓟ Ⓟ Ⓦ

Immunizations
Ⓟ Ⓟ Ⓟ Ⓟ Ⓟ Ⓟ Ⓟ

Lab results
Ⓟ Ⓟ Ⓟ Ⓟ Ⓟ Ⓢ Ⓟ Ⓦ

Medication administrations
Ⓢ Ⓢ Ⓢ Ⓢ Ⓢ Ⓢ

Medication dispensations
Ⓢ Ⓢ Ⓢ Ⓢ Ⓢ Ⓢ

Medication orders
Ⓟ Ⓟ Ⓟ Ⓟ Ⓟ Ⓟ Ⓟ

Medication statements
Ⓟ Ⓟ Ⓟ Ⓟ Ⓟ Ⓟ Ⓟ

Patient documents
Ⓟ Ⓟ Ⓟ Ⓟ Ⓟ Ⓟ Ⓦ

Patient demographics
Ⓟ Ⓟ Ⓟ Ⓟ Ⓟ Ⓟ

Problems
Ⓟ Ⓟ Ⓟ Ⓟ Ⓟ Ⓟ Ⓦ

Procedures
Ⓟ Ⓟ Ⓟ Ⓟ Ⓟ Ⓟ Ⓦ

Smoking status
Ⓟ Ⓟ Ⓟ Ⓟ Ⓟ Ⓟ Ⓦ

Vital signs
Ⓟ Ⓟ Ⓟ Ⓟ Ⓟ Ⓟ Ⓦ

Implements all the S4S requirements
Ⓟ Ⓟ Ⓟ Ⓟ Ⓟ Ⓟ Ⓟ Ⓟ Ⓟ Ⓟ

App asks for authorization
Ⓟ Ⓟ Ⓟ Ⓟ Ⓟ Ⓟ Ⓟ Ⓟ

EHR evaluates authorization request
Ⓟ Ⓟ Ⓟ Ⓟ

App exchanges authorization code for access token
Ⓟ Ⓟ Ⓟ Ⓟ Ⓟ Ⓟ Ⓟ Ⓟ

App uses a refresh token to obtain a new access token
Ⓟ Ⓟ Ⓟ

User revokes authorization
Ⓟ

Pro tip! Use keyboard n (next) and p (prev) to cycle through failure reports.

Tests Complete!

Feature: Allergies and intolerances ✗

allergies-and-intolerances

Scenario: Correct resourceType

Given I have a Allergies and intolerances response ✓
Then the resourceType field will be Bundle ✓
Then the type field will be searchset ✓

Scenario: Resources are valid FHIR content

Given I have a Allergies and intolerances response ✓
Then the resource parses as valid FHIR DSTU2 content ✓

Scenario: Results exist

Given I have a Allergies and intolerances response ✓
Then there should be at least 1 entry ✓

Scenario: Resources have ids

Given I have a Allergies and intolerances response ✓
And there is at least 1 entry ✓
Then all resources will have a id field ✓

Scenario: All references will resolve

Given I have a Allergies and intolerances response ✓
And there is at least 1 entry ✓
Then all references will resolve ✓

Scenario: All the codes are valid

Given I have a Allergies and intolerances response ✓
And there is at least 1 entry ✓
Then all the codes will be valid ✓

Scenario: Resources fulfill the Argonaut Allergies profile

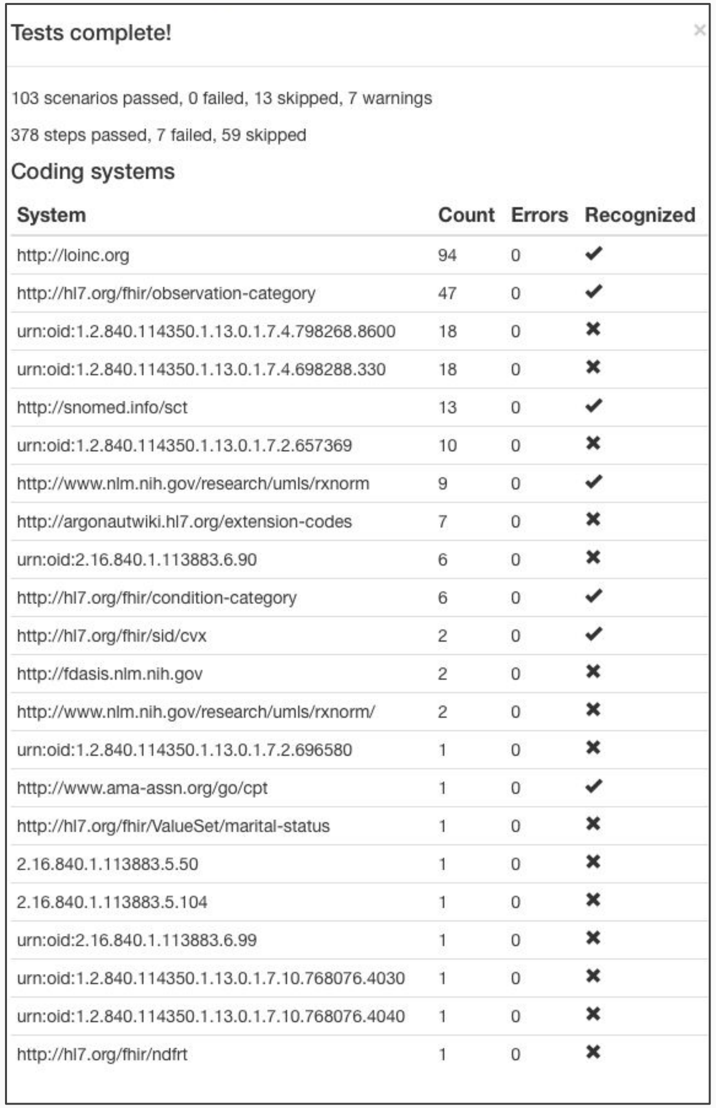
warning

Given I have a Allergies and intolerances response ✓
And there is at least 1 entry ✓
Then there exists one Identification of a substance, or a class of substances, that is considered to be responsible for the adverse reaction risk in AllergyIntolerance.substance ✓
Then there exists one reference to a Patient in AllergyIntolerance.patient ✗

```
Assertion Failed: https://open-ic.epic.com/Argonaut/api/FHIR/Argonaut/Patient/Tbt3KuCY

Request
-------
GET https://open-ic.epic.com/Argonaut/api/FHIR/Argonaut/AllergyIntolerance?patient=Tbt
User-Agent: python-requests/2.10.0
Accept-Encoding: deflate,sdch
Connection: keep-alive
Accept: application/json
Authorization: Bearer Qs3VBFWgSG9HioqedJ/1Ee6xa24RbmwNabGwI9mVDUcxsNudDkgqbPU7EDTK9Azs

Response
--------
Cache-Control: no-cache
Pragma: no-cache
Content-Length: 4024
Content-Type: application/json; charset=utf-8
Expires: -1
Server: Microsoft-IIS/8.5
```



Tests complete!

103 scenarios passed, 0 failed, 13 skipped, 7 warnings

378 steps passed, 7 failed, 59 skipped

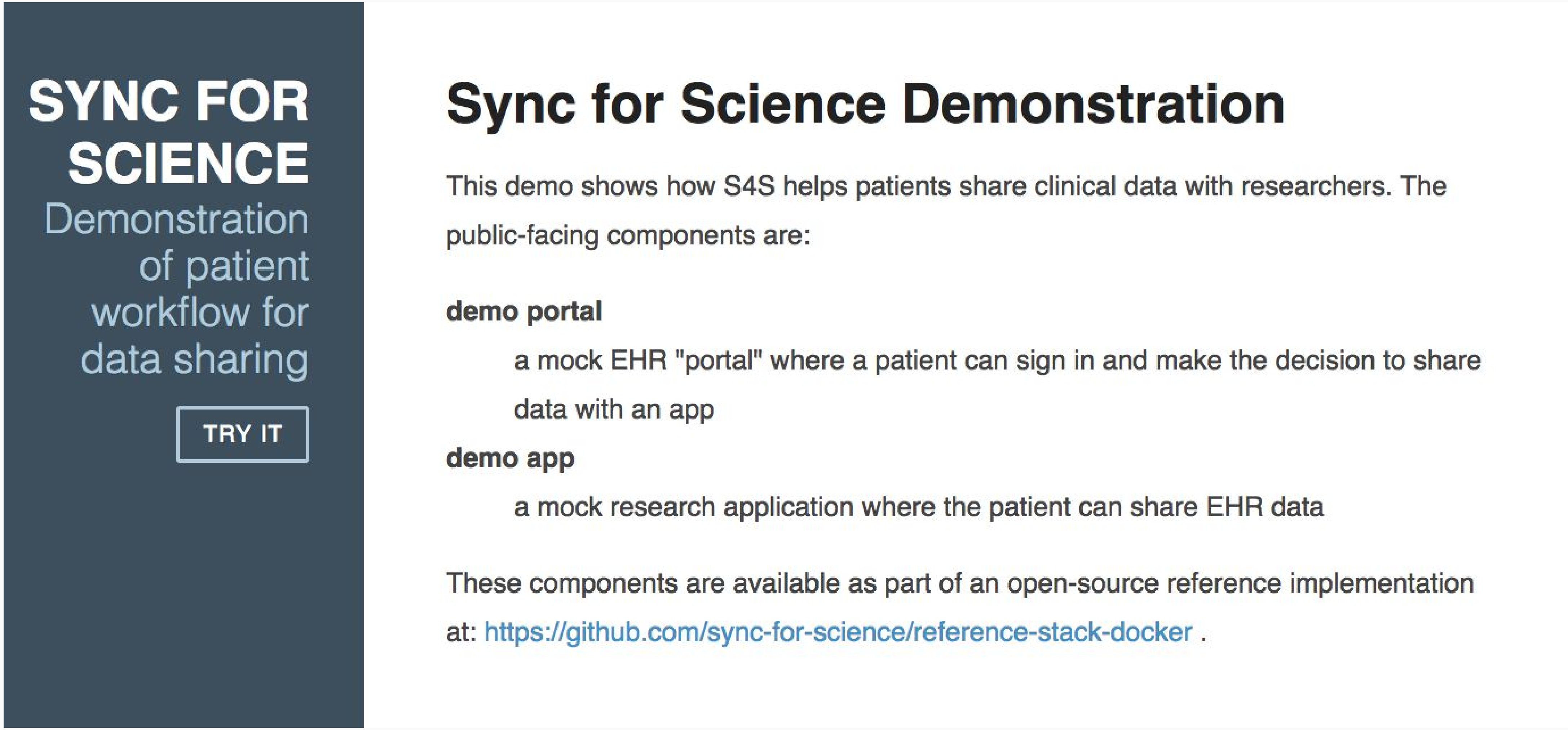
Coding systems

System	Count	Errors	Recognized
http://loinc.org	94	0	✓
http://hl7.org/fhir/observation-category	47	0	✓
urn:oid:1.2.840.114350.1.13.0.1.7.4.798268.8600	18	0	✗
urn:oid:1.2.840.114350.1.13.0.1.7.4.698288.330	18	0	✗
http://snomed.info/sct	13	0	✓
urn:oid:1.2.840.114350.1.13.0.1.7.2.657369	10	0	✗
http://www.nlm.nih.gov/research/umls/rxnorm	9	0	✓
http://argonautwiki.hl7.org/extension-codes	7	0	✗
urn:oid:2.16.840.1.113883.6.90	6	0	✗
http://hl7.org/fhir/condition-category	6	0	✓
http://hl7.org/fhir/sid/cvx	2	0	✓
http://fdasis.nlm.nih.gov	2	0	✗
http://www.nlm.nih.gov/research/umls/rxnorm/	2	0	✗
urn:oid:1.2.840.114350.1.13.0.1.7.2.696580	1	0	✗
http://www.ama-assn.org/go/cpt	1	0	✓
http://hl7.org/fhir/ValueSet/marital-status	1	0	✗
2.16.840.1.113883.5.50	1	0	✗
2.16.840.1.113883.5.104	1	0	✗
urn:oid:2.16.840.1.113883.6.99	1	0	✗
urn:oid:1.2.840.114350.1.13.0.1.7.10.768076.4030	1	0	✗
urn:oid:1.2.840.114350.1.13.0.1.7.10.768076.4040	1	0	✗
http://hl7.org/fhir/ndfrt	1	0	✗

Demo
Src

Research App – Demonstration

SYNC FOR SCIENCE



SYNC FOR SCIENCE
Demonstration of patient workflow for data sharing

Sync for Science Demonstration

This demo shows how S4S helps patients share clinical data with researchers. The public-facing components are:

demo portal
a mock EHR "portal" where a patient can sign in and make the decision to share data with an app

demo app
a mock research application where the patient can share EHR data

These components are available as part of an open-source reference implementation at: https://github.com/sync-for-science/reference-stack-docker .

Demo
Src

Related Work

SMART on FHIR	bit.ly/smart-fhir-2017, gallery.smarthealthit.org
API Privacy and Security	Taskforce report
Argonaut Project	github.com/argonautproject
FHIR	hl7.org/fhir
CDS Hooks	cds-hooks.org

SMART C-CDA Scorecard, Analysis, Samples (2013)
bit.ly/ccda-webinar, jamia.oxfordjournals.org/content/21/6/1060