Building Consumer Access Apps

Jennifer Hong

Senior Software Engineer

November 12, 2020

Empowering beyond

Cerner

Consumer Apps

Who and How

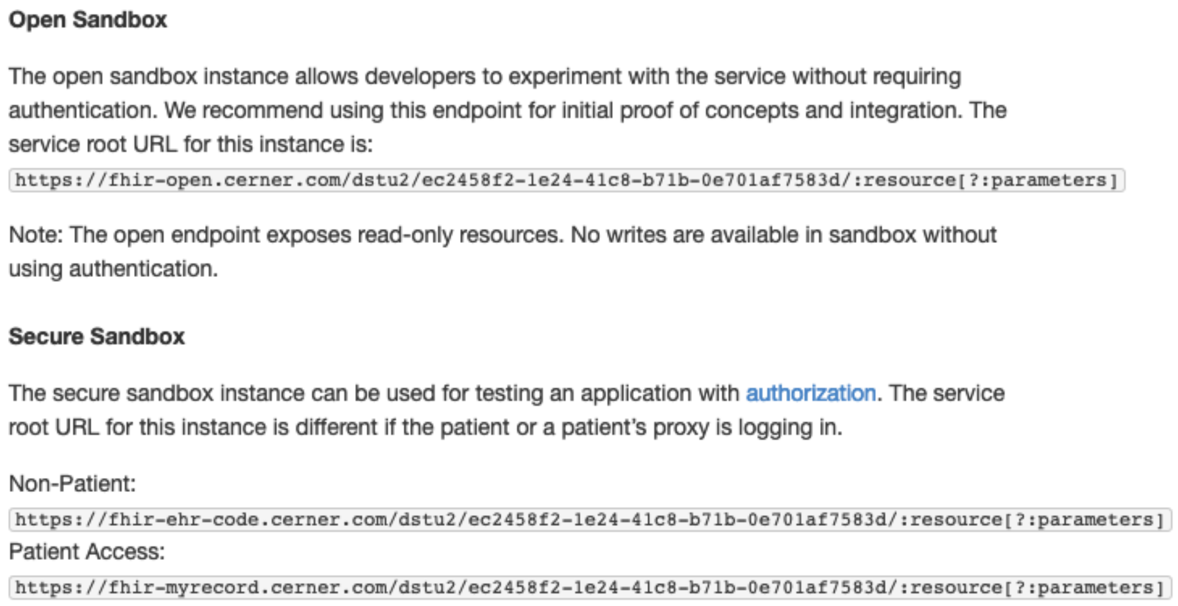
- **Accessed by patients or their authorized representatives**
- Not clinicians
- **Off hospital network**

Authorization

Authorization

Workflow

- **Workflow from an *app* perspective is the same**
  - The FHIR server root URL is different
  - https://fhir.cerner.com/millennium/dstu2/#service-root-url



Open Sandbox

The open sandbox instance allows developers to experiment with the service without requiring authentication. We recommend using this endpoint for initial proof of concepts and integration. The service root URL for this instance is:

```
https://fhir-open.cerner.com/dstu2/ec2458f2-1e24-41c8-b71b-0e701af7583d/:resource[?:parameters]
```

Note: The open endpoint exposes read-only resources. No writes are available in sandbox without using authentication.

Secure Sandbox

The secure sandbox instance can be used for testing an application with authorization. The service root URL for this instance is different if the patient or a patient's proxy is logging in.

Non-Patient:

```
https://fhir-ehr-code.cerner.com/dstu2/ec2458f2-1e24-41c8-b71b-0e701af7583d/:resource[?:parameters]
```

Patient Access:

```
https://fhir-myrecord.cerner.com/dstu2/ec2458f2-1e24-41c8-b71b-0e701af7583d/:resource[?:parameters]
```

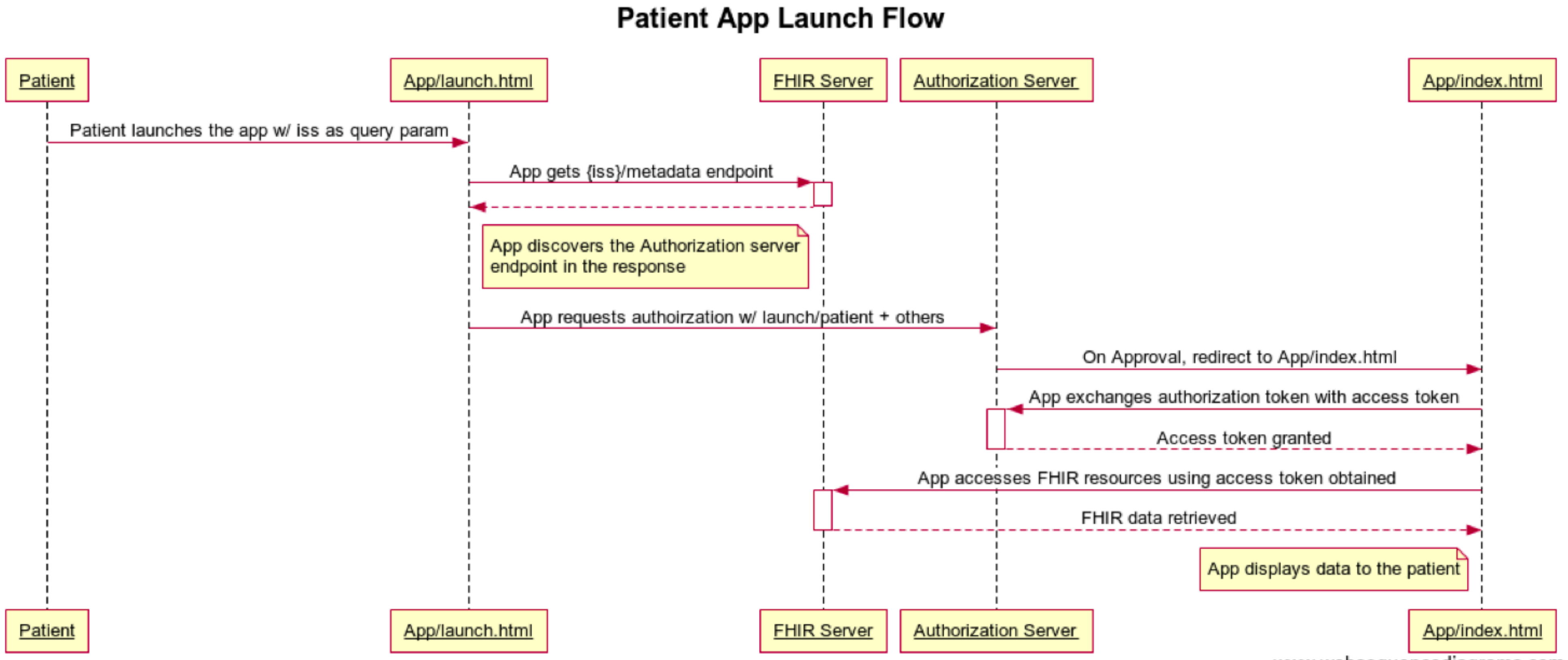
Authorization Workflow

Introduction Talks

- “Introduction to SMART on FHIR” Today at 12:30 pm
- “SMART on FHIR Authorization” Today at 1:30 pm

Authorization Workflow

Launch Demo



Patient App Launch Flow

Patient launches the app w/ iss as query param

App gets {iss}/metadata endpoint

App discovers the Authorization server endpoint in the response

App requests authoirzation w/ launch/patient + others

On Approval, redirect to App/index.html

App exchanges authorization token with access token

Access token granted

App accesses FHIR resources using access token obtained

FHIR data retrieved

App displays data to the patient

www.websequencediagrams.com

Authorization

SMART Scopes

- **launch (launch from portal)**
- **launch/patient (not supported currently for practitioners)**
  - User will get prompted to choose a patient
  - MUST for standalone apps that use the SMART patient-specific scopes
    - EG: patient/AllergyIntolerance.read
- **online_access**
  - Allows the app to obtain a new token while the end-user remains online
- **offline_access (not supported currently for practitioners)**
  - Allows the app to obtain a new token even after the end-user is no longer online
  - Requires confidential client

Authorization

Who?

- **Patient/self**
- **Patient authorized representative**
  - Spouse
  - Parent
  - Caretakers
  - Etc.
- **Same authentication credentials as portal login**

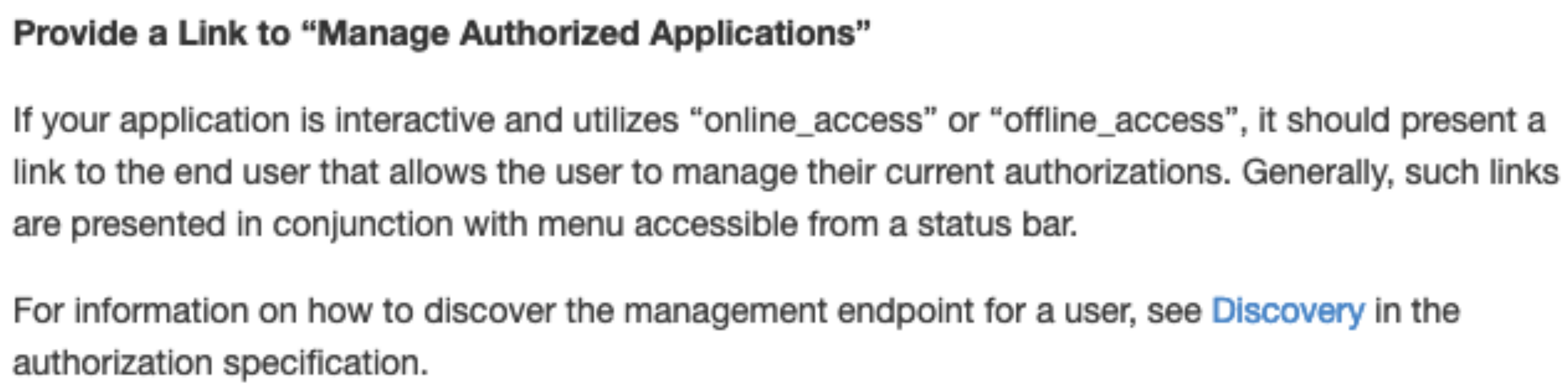
Authorization

Offline Access Special Considerations

- **Offline access is long term**
  - App accesses while patient is no longer signed in
  - EG: step trackers
- **There is a management URL in the authorization section of the Conformance/CapabilityStatement resource (/metadata)**
  - This URL should be accessible from within your application

Manage URL

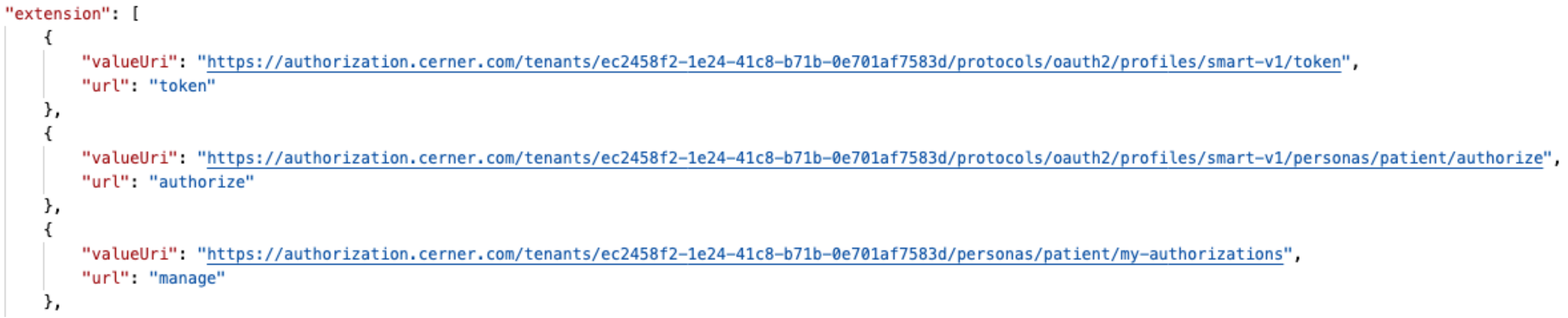
https://fhir.cerner.com/authorization/#user-experience



Provide a Link to “Manage Authorized Applications”

If your application is interactive and utilizes “online_access” or “offline_access”, it should present a link to the end user that allows the user to manage their current authorizations. Generally, such links are presented in conjunction with menu accessible from a status bar.

For information on how to discover the management endpoint for a user, see Discovery in the authorization specification.



```
"extension": [
    {
        "valueUri": "https://authorization.cerner.com/tenants/ec2458f2-1e24-41c8-b71b-0e701af7583d/protocols/oauth2/profiles/smart-v1/token",
        "url": "token"
    },
    {
        "valueUri": "https://authorization.cerner.com/tenants/ec2458f2-1e24-41c8-b71b-0e701af7583d/protocols/oauth2/profiles/smart-v1/personas/patient/authorize",
        "url": "authorize"
    },
    {
        "valueUri": "https://authorization.cerner.com/tenants/ec2458f2-1e24-41c8-b71b-0e701af7583d/personas/patient/my-authorizations",
        "url": "manage"
    },
```

Data Access

Data Access

Patient Data Access Concerns

- **Like practitioners, there are privacy and security concerns**
  - IE Not all users have access to all data
- **This may vary user to user and site to site**
- **This is enforced by the API**
- **The app (and user) will not know when there may be data available that cannot be seen**
- **Laws**
  - Adolescent proxy: both age range and what may be restricted from a parent may vary by site or state

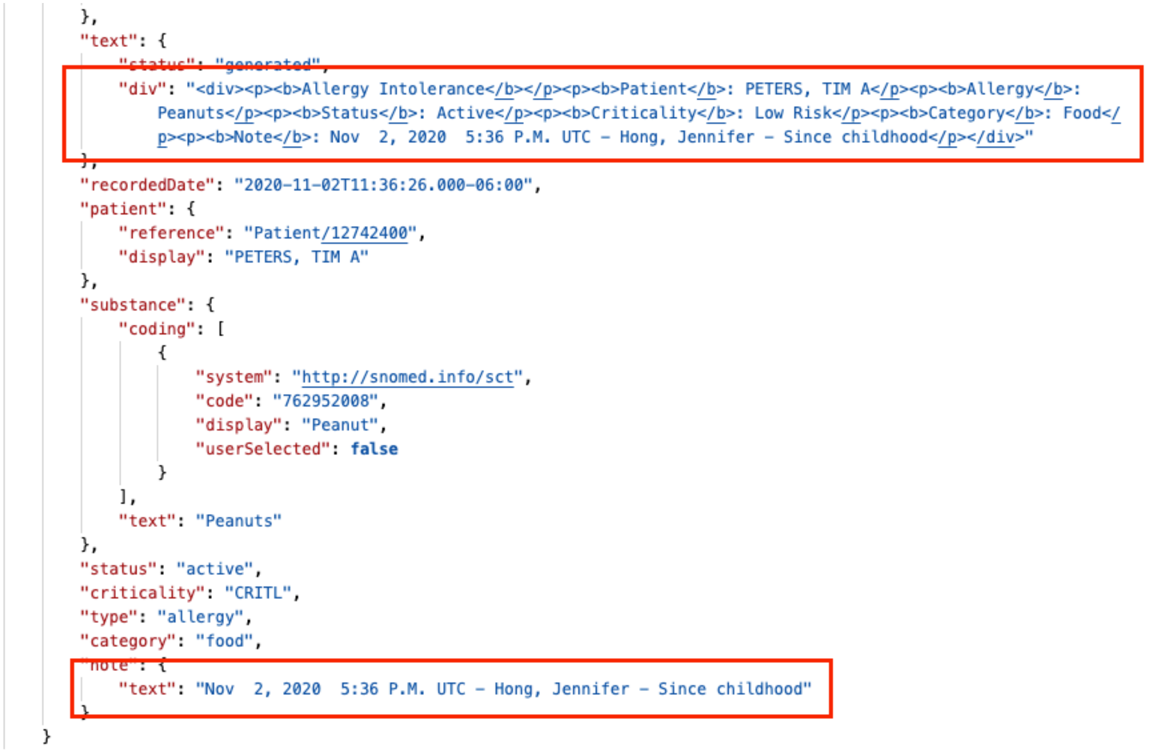
Data Access

Masked Fields

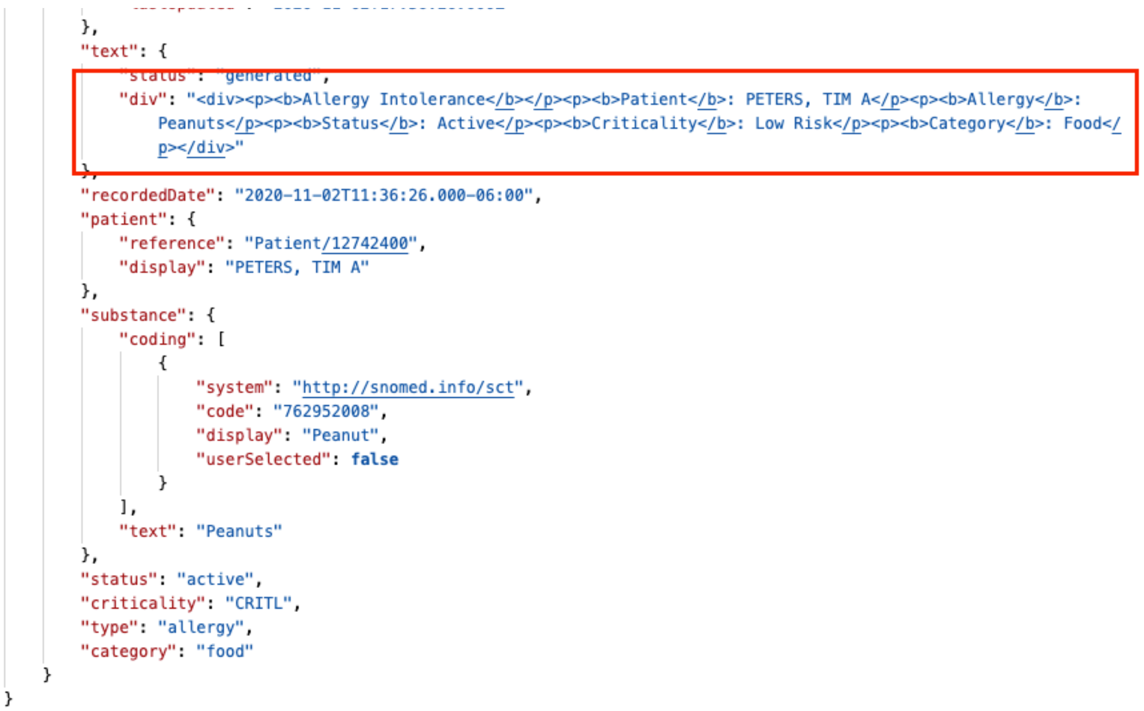
- **Some fields may be masked**
- **This can be true for all consumer users**
  - EG: Comments that are often administrative
- **This can be true for only some consumer users**
  - EG: The adolescent proxy use case
- **This can be true for certain statuses**

Masked Fields

Notes Example



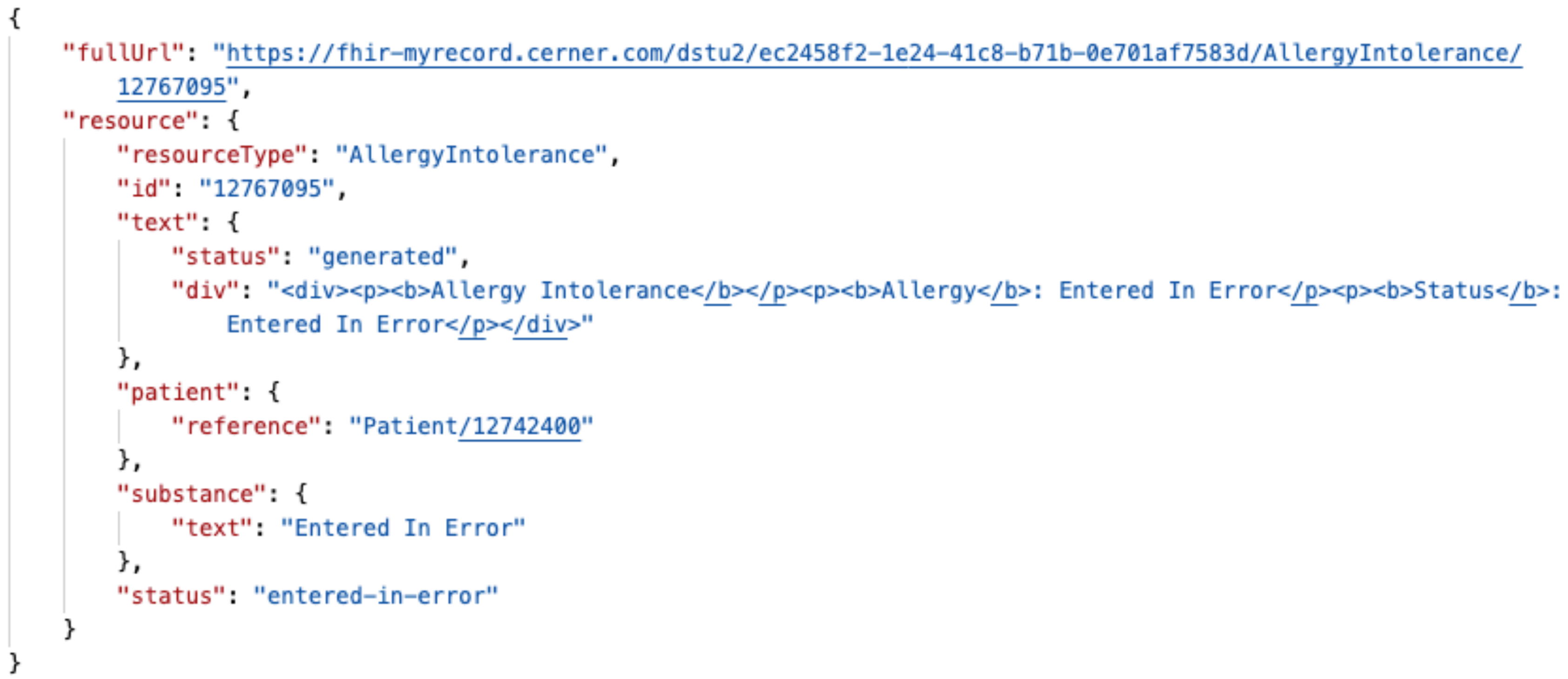
```
    },
    "text": {
        "status": "generated",
        "div": "<div><p><b>Allergy Intolerance</b></p><p><b>Patient</b>: PETERS, TIM A</p><p><b>Allergy</b>:
            Peanuts</p><p><b>Status</b>: Active</p><p><b>Criticality</b>: Low Risk</p><p><b>Category</b>: Food</
            p><p><b>Note</b>: Nov  2, 2020  5:36 P.M. UTC - Hong, Jennifer - Since childhood</p></div>"
    },
    "recordedDate": "2020-11-02T11:36:26.000-06:00",
    "patient": {
        "reference": "Patient/12742400",
        "display": "PETERS, TIM A"
    },
    "substance": {
        "coding": [
            {
                "system": "http://snomed.info/sct",
                "code": "762952008",
                "display": "Peanut",
                "userSelected": false
            }
        ],
        "text": "Peanuts"
    },
    "status": "active",
    "criticality": "CRITL",
    "type": "allergy",
    "category": "food",
    "note": {
        "text": "Nov  2, 2020  5:36 P.M. UTC - Hong, Jennifer - Since childhood"
    }
}
```



```
    },
    "text": {
        "status": "generated",
        "div": "<div><p><b>Allergy Intolerance</b></p><p><b>Patient</b>: PETERS, TIM A</p><p><b>Allergy</b>:
            Peanuts</p><p><b>Status</b>: Active</p><p><b>Criticality</b>: Low Risk</p><p><b>Category</b>: Food</
            p></div>"
    },
    "recordedDate": "2020-11-02T11:36:26.000-06:00",
    "patient": {
        "reference": "Patient/12742400",
        "display": "PETERS, TIM A"
    },
    "substance": {
        "coding": [
            {
                "system": "http://snomed.info/sct",
                "code": "762952008",
                "display": "Peanut",
                "userSelected": false
            }
        ],
        "text": "Peanuts"
    },
    "status": "active",
    "criticality": "CRITL",
    "type": "allergy",
    "category": "food"
  }
}
```

Masked Fields

Entered In Error Status Example



```
{
    "fullUrl": "https://fhir-myrecord.cerner.com/dstu2/ec2458f2-1e24-41c8-b71b-0e701af7583d/AllergyIntolerance/
        12767095",
    "resource": {
        "resourceType": "AllergyIntolerance",
        "id": "12767095",
        "text": {
            "status": "generated",
            "div": "<div><p><b>Allergy Intolerance</b></p><p><b>Allergy</b>: Entered In Error</p><p><b>Status</b>:
                Entered In Error</p></div>"
        },
        "patient": {
            "reference": "Patient/12742400"
        },
        "substance": {
            "text": "Entered In Error"
        },
        "status": "entered-in-error"
    }
}
```

Data Access

Masked Resources

- **Some content may have been deemed not available to consumers by site policy or state law**
- **May not be available to any consumer (self or proxy)**
  - EG Administrative tasks, HIV status
- **May not be available to specific classes of consumers**
  - EG Pregnancy status not exposed to an adolescent’s parents

Data Access

Masked Resources

- **The big takeaway: Absence of data doesn’t mean “negation”**
  - IE Absence of pregnancy or HIV results doesn’t mean there wasn’t one
- **If the app needs this data to work safely, it may need to confirm with the user**

Other API Differences

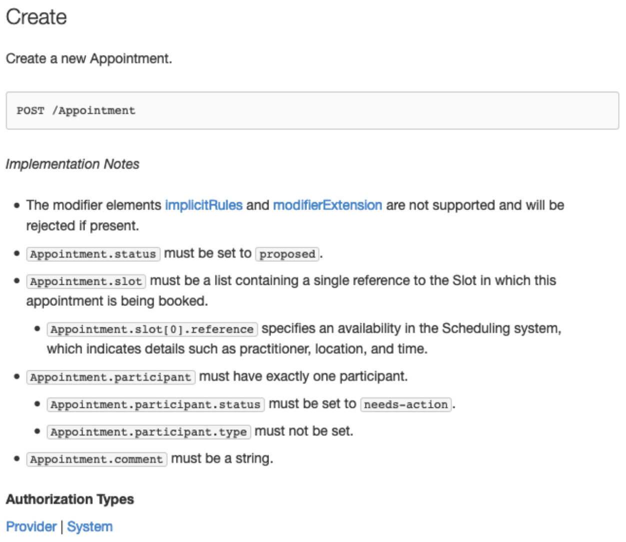
Other API Differences

Writes

- **Writes currently aren’t available**
  - Future investigation
  - Argonaut/HL7 also thinking through these workflows
- **For scheduling: Currently use a B2B/system account**
  - Chicken/egg of patient self-registering vs having a portal login
  - Allows addition of basic patient demographics and appointment
  - This is specific to scheduling workflows, B2B isn’t a “workaround” for other writes

Source Of Truth

- **All of these action level / resource level differences are available in Conformance and CapabilityStatement and documentation**
- **Documentation: Authorization Types section**
  - https://fhir.cerner.com/millennium/dstu2/scheduling/appointment/#create
  - https://fhir.cerner.com/millennium/dstu2/scheduling/appointment/#search (available for patients)



Create

Create a new Appointment.

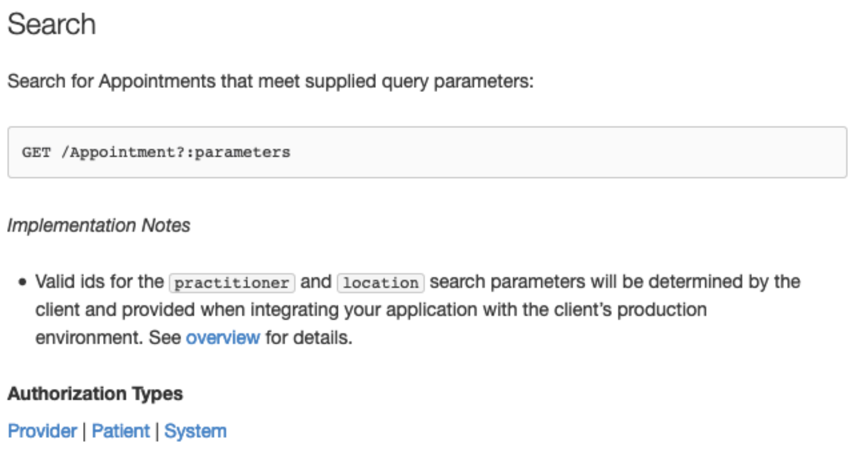
```
POST /Appointment
```

Implementation Notes

- The modifier elements implicitRules and modifierExtension are not supported and will be rejected if present.
- `Appointment.status` must be set to `proposed`.
- `Appointment.slot` must be a list containing a single reference to the Slot in which this appointment is being booked.
  - `Appointment.slot[0].reference` specifies an availability in the Scheduling system, which indicates details such as practitioner, location, and time.
- `Appointment.participant` must have exactly one participant.
  - `Appointment.participant.status` must be set to `needs-action`.
  - `Appointment.participant.type` must not be set.
- `Appointment.comment` must be a string.

Authorization Types

Provider | System



Search

Search for Appointments that meet supplied query parameters:

```
GET /Appointment?:parameters
```

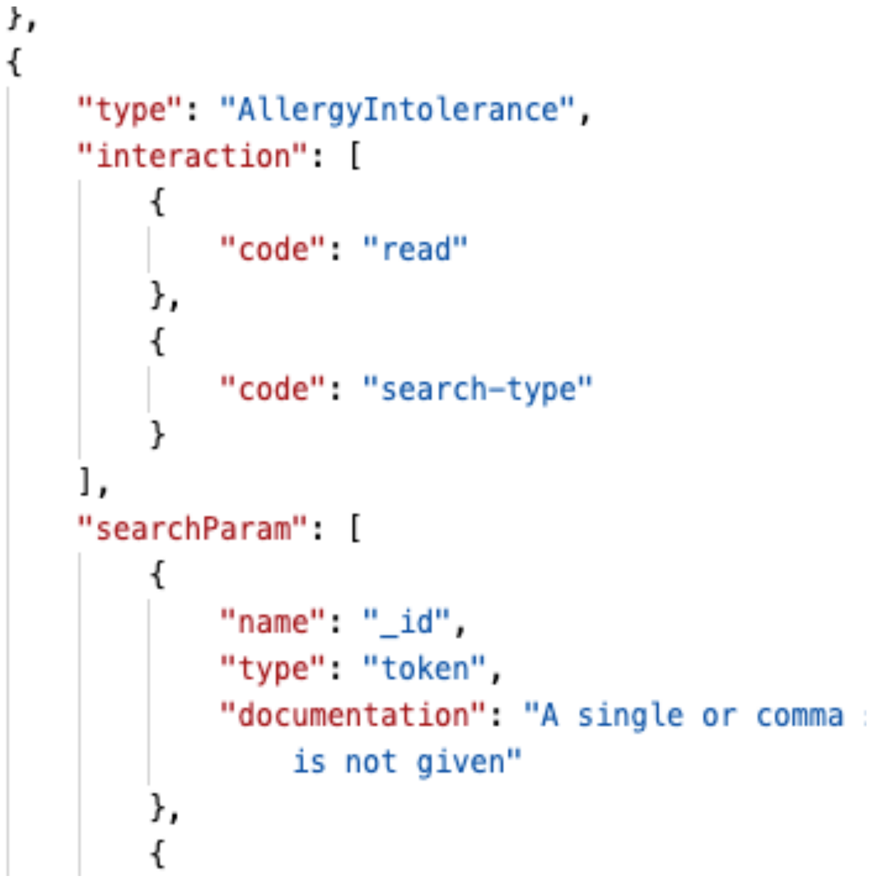
Implementation Notes

- Valid ids for the `practitioner` and `location` search parameters will be determined by the client and provided when integrating your application with the client's production environment. See overview for details.

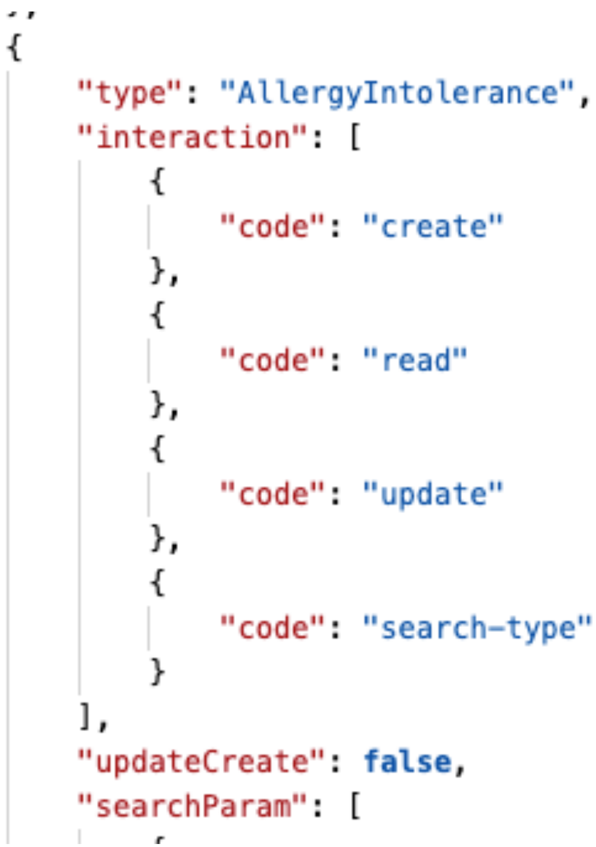
Authorization Types

Provider | Patient | System

Capability Statement / Conformance



```
},
{
    "type": "AllergyIntolerance",
    "interaction": [
        {
            "code": "read"
        },
        {
            "code": "search-type"
        }
    ],
    "searchParam": [
        {
            "name": "_id",
            "type": "token",
            "documentation": "A single or comma
                is not given"
        },
        {
```



```
},
{
    "type": "AllergyIntolerance",
    "interaction": [
        {
            "code": "create"
        },
        {
            "code": "read"
        },
        {
            "code": "update"
        },
        {
            "code": "search-type"
        }
    ],
    "updateCreate": false,
    "searchParam": [
        {
```

Other Considerations

Other Considerations

Privacy Concerns

- **The patient is handing over their health information**
- **App should provide easy access to:**
  - Who to contact for support / How to get support
  - What data the app uses and how it uses this data?
  - Where the data is stored, sent, or shared?
    - EG Is this going to stay on your own servers for research?
  - Who will have access to the data?
  - Will the data be de-identified?

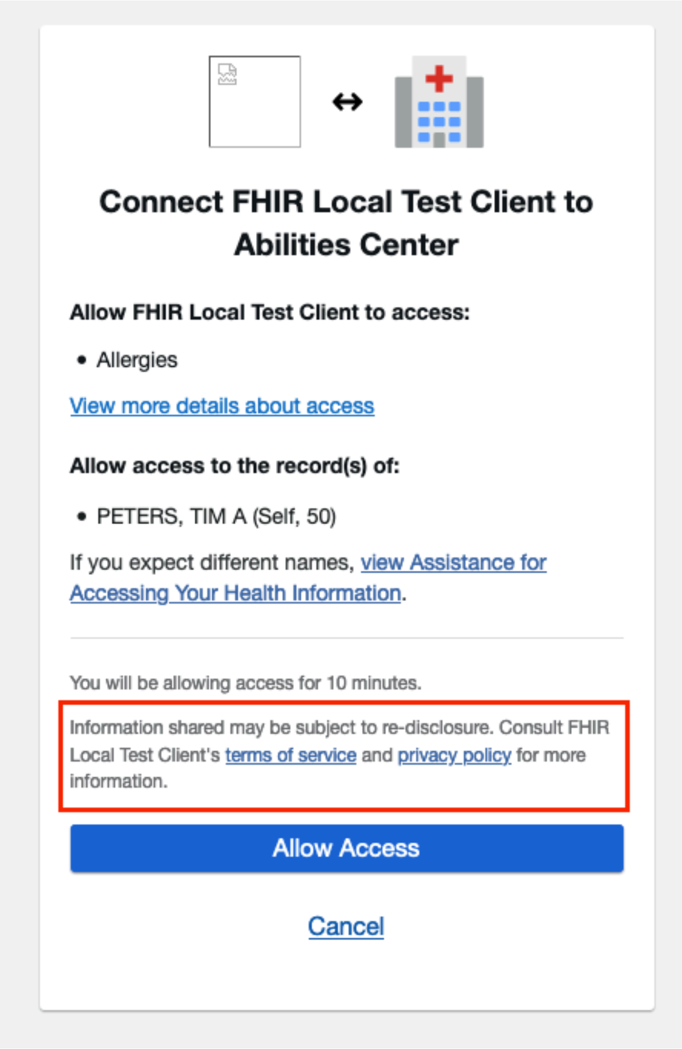
Other Considerations

Privacy Concerns

- Privacy policy URL can be provided and included on the authorization page
- Terms of Service can be provided and included on the authorization page
- Breach notifications?

Privacy Concerns

Terms of Service and Privacy Policy Example



Connect FHIR Local Test Client to Abilities Center

Allow FHIR Local Test Client to access:

- Allergies

View more details about access

Allow access to the record(s) of:

- PETERS, TIM A (Self, 50)

If you expect different names, view Assistance for Accessing Your Health Information.

You will be allowing access for 10 minutes.

Information shared may be subject to re-disclosure. Consult FHIR Local Test Client's terms of service and privacy policy for more information.

Code Program and Onboarding

Onboarding

code Program

Membership is *not* required if the app uses only the common clinical data set reads/searches

- AllergyIntolerance
- CarePlan (team and plan)
- Condition
- Device
- DocumentReference
- Goal
- Immunization
- MedicationOrder
- MedicationStatement
- Patient
- Procedure
- Observation
  - Labs
  - Vitals
  - Social History / Smoking

Onboarding

Taking it to Prod

- **Basic company details**
  - Company details
  - Business contacts
  - Support contacts
- **TOS and Privacy policy URLs**
- **Normal app registration details (redirect/launch, scopes, etc.)**
- **Helps clients find help**
- **Helps us contact you in case of issues**

Onboarding

Taking it to Prod cont.

- **CCDS apps are not listed in our App gallery**
- **Registered CCDS apps are listed on a client accessible page as options to whitelist**
- **Once registered and ready, you contact clients**
- **Clients log a simple service request to whitelist your app in their environment**

Onboarding

Validation?

- **Part of the code program, but not required for CCDS access**
- **Can pay a validation fee to get validated and listed in our app gallery**
- **Validation improves quality!**

Learn More

Tutorial

Tutorial Demo

- https://engineering.cerner.com/smart-on-fhir-tutorial/#introduction
- https://engineering.cerner.com/smart-on-fhir-tutorial/#patient-app
- https://engineering.cerner.com/smart-on-fhir-tutorial/#standalone-app-launch-for-patient-access-workflow

Learn More

Other Talks

- **Introduction to SMART on FHIR – Today at 12:30 pm**
- **Building a Scheduling App – Today at 12:30 pm**
- **SMART on FHIR Authorization – Today at 1:30 pm**
- **Best Practices for App Integration – Today at 3:30 pm**
- **Troubleshooting SMART/FHIR – Today at 2:30 pm**
- **Putting It All Together – Tomorrow at 9:00 am**

Questions?