Computing for Medicine

Lecture 11: HL7 & FHIR

Step 3: Choose a Technical Framework, e.g. FHIR

What we want

Report from Lab123457, 15:30 14-Aug-2008, Ref 123456789

Patient: MICKEY MOUSE, DoB: 14-Jan-1962, M

Address: 14 Disney Rd, Disneyland, MM1 9DL

Specimen: Swab, FOOT, Right, Requested By: C987654

Location: 5 N

Patients GP: Dr Smith (G123456)

Organism: STAU

Susceptibility:	AMP	R
	SXT	S
	CIP	S

What it looks like at the backend

```
MSH|^~\&||^123457^Labs|||200808141530||ORU^R01|12345678
  9|P|2.4
PID|||123456^^^SMH^PI||MOUSE^MICKEY||19620114|M|||14
  Disney Rd^Disneyland^^^MM1 9DL
PV1|||5 N|||||G123456^DR SMITH
OBR|||54321|666777^CULTURE^LN|||20080802|||||||SW^^^FOO
  T^RT|C987654
OBX||CE|0^ORG|01|STAU||||||F
OBX||CE|500152^AMP|01||||R|||F
OBX||CE|500155^SXT|01||||S|||F
OBX||CE|500162^CIP|01||||S|||F
```

Technical Interoperability: The Technology Layer

This is the technology layer

- Moves data from system A to system B, neutralizing the effects of distance
- Domain independent
- Does not know or care about the meaning of what is exchanged
- Information theory is the foundation stone of technical interoperability

Health Level 7 International (HL7)

- Is a Standards Development Organization
- Is now the lingua franca to pass health messages across systems
- At least two translations required during information interchange

Internal format	--->	Wire Format	--->	Internal Format
(computer)		(connection)		(computer)

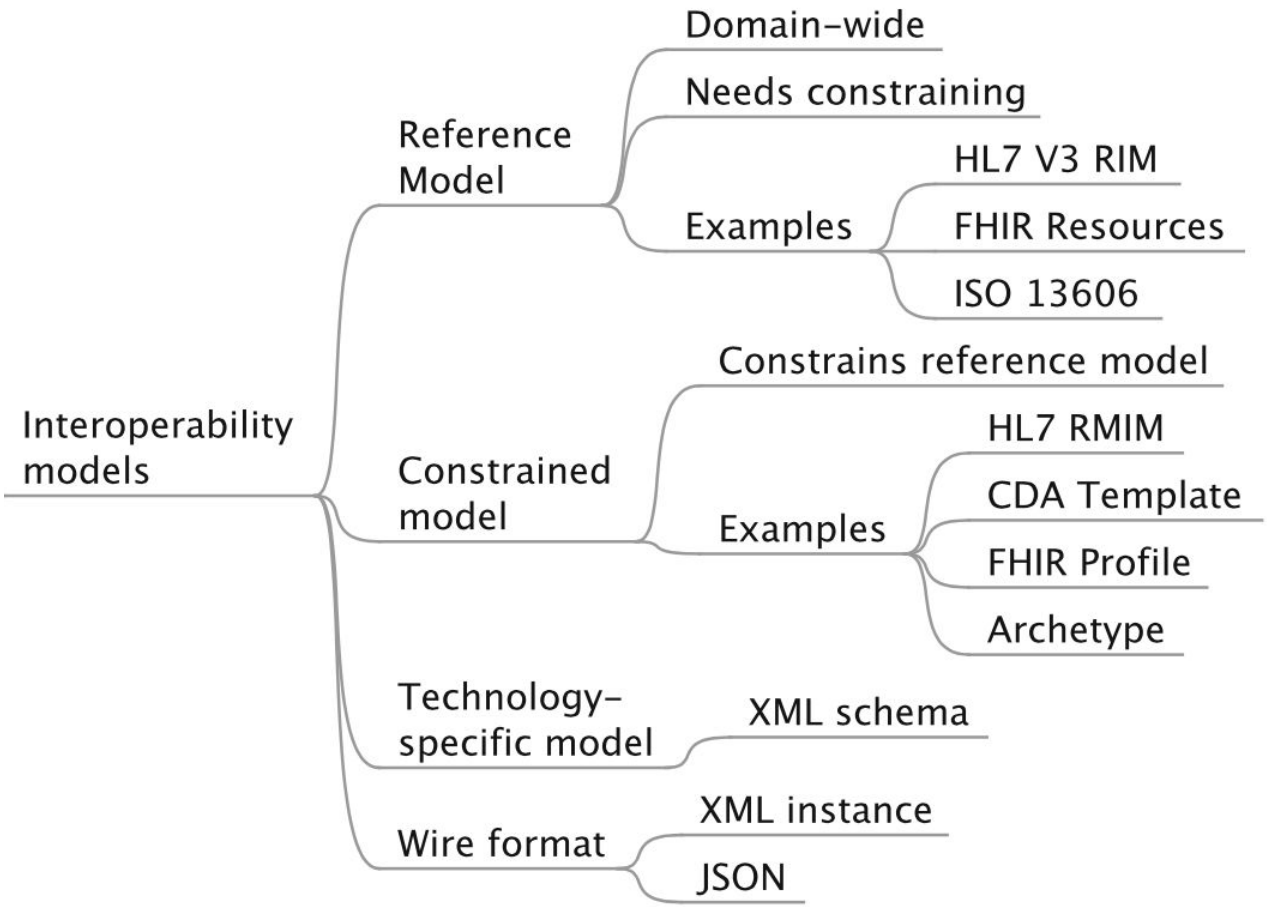
Requires the following sequential steps in Object Oriented Software Development

i. Computational-Independent Model (CIM).
ii. Platform-Independent Model (PIM) - the conceptual design of a system.
iii. Platform-Specific Model (PSM)- the implementable design.
iv. Code, the actual software code, also referred to as wire-format.

Another Example of Syntactic Interoperability: HL7 Standard

```
##### Translate this function from HL7 V2.8 ADT_A01 to HL7 V2.4 ADT_A05
### HL7 V2.8 ADT_A01
```

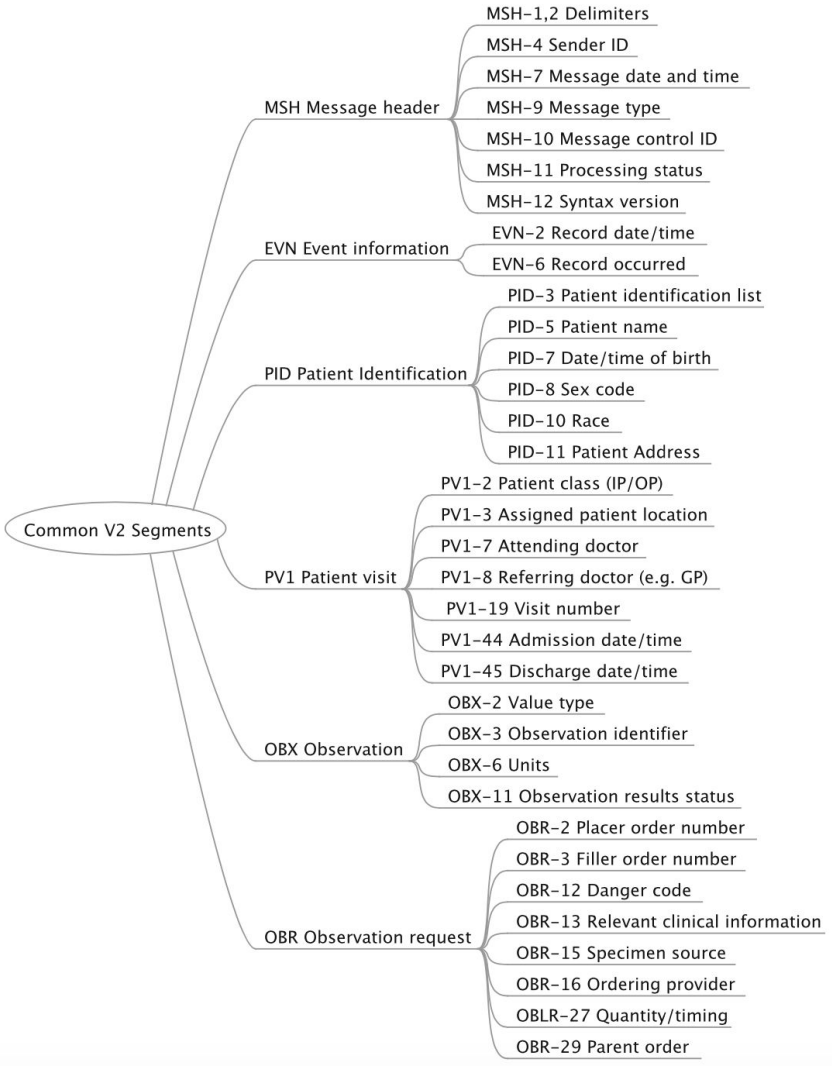
```
    MSH|^~\&|ADT1|GOOD HEALTH HOSPITAL|GHH LAB, INC.|GOOD HEALTH
HOSPITAL|198808181126|SECURITY|ADT^A01^ADT_A01|MSG00001|P|2.8||
    EVN|A01|200708181123||
    PID|1||PATID1234^5^M11^ADT1^MR^GOOD HEALTH
HOSPITAL~123456789^^^USSSA^SS||EVERYMAN^ADAM^A^III||19610615|M||C|222
2 HOME STREET^^GREENSBORO^NC^27401-1020|GL|(555) 555-2004|(555)555-
2004||S||PATID12345001^2^M10^ADT1^AN^A|444333333|987654^NC|
    NK1|1|NUCLEAR^NELDA^W|SPO^SPOUSE||||NK^NEXT OF KIN
    PV1|1|I|2000^2012^01||||004777^ATTEND^AARON^A|||SUR||||ADM|A0|

### HL7 V2.4 ADT_A05
```


Interoperability models
Reference Model
Domain-wide
Needs constraining
Examples
HL7 V3 RIM
FHIR Resources
ISO 13606
Constrained model
Constrains reference model
Examples
HL7 RMIM
CDA Template
FHIR Profile
Archetype
Technology-specific model
XML schema
Wire format
XML instance
JSON

Segment Definitions, Segments, Reports

```
MSH|^~\&||^123457^Labs|||200808141530||ORU^R01|12345678
  9|P|2.4
PID|||123456^^^SMH^PI||MOUSE^MICKEY||19620114|M|||14
  Disney Rd^Disneyland^^^MM1 9DL
PV1|||5 N|||||G123456^DR SMITH
OBR|||54321|666777^CULTURE^LN|||20080802|||||||SW^^^FOO
  T^RT|C987654
OBX||CE|0^ORG|01|STAU|||||F
OBX||CE|500152^AMP|01||||R|||F
OBX||CE|500155^SXT|01||||S|||F
OBX||CE|500162^CIP|01||||S|||F
```

Report from Lab123457, 15:30 14-Aug-2008, Ref 123456789		
Patient: MICKEY MOUSE, DoB: 14-Jan-1962, M		
Address: 14 Disney Rd, Disneyland, MM1 9DL		
Specimen: Swab, FOOT, Right, Requested By: C987654		
Location: 5 N		
Patients GP: Dr Smith (G123456)		
Organism: STAU		
Susceptibility:	AMP	R
	SXT	S
	CIP	S



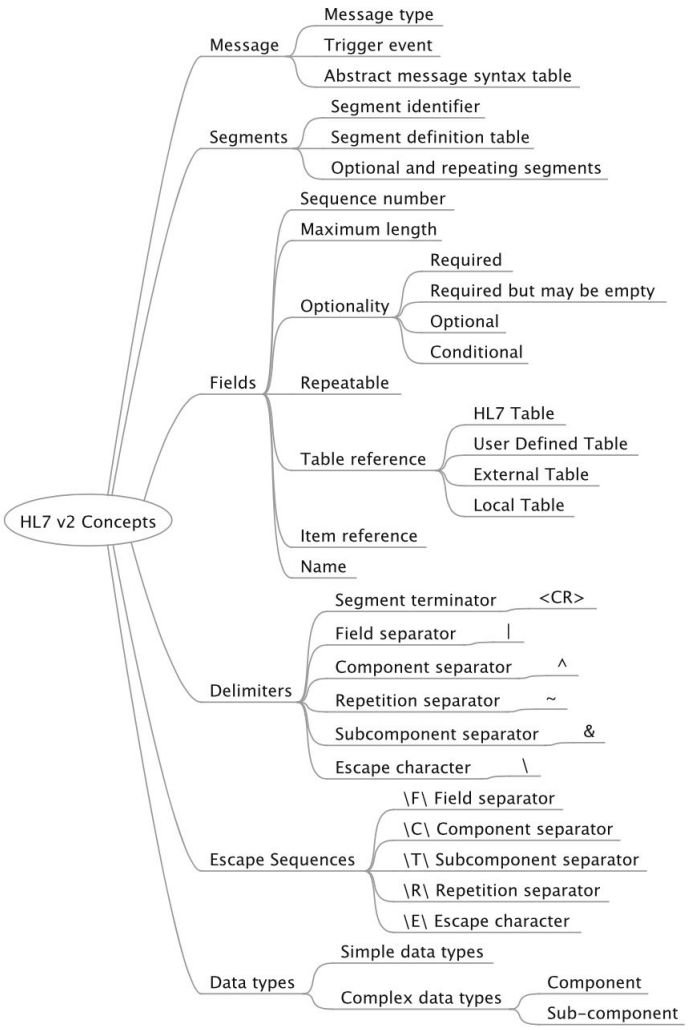
HL7 Messages

Value	Description
ACK	General acknowledgment message
ADT	ADT message
ORM	Order message
ORU	Observation result unsolicited

Value	Description
A01	Admit/visit notification
A02	Transfer a patient
A03	Discharge/end visit
A04	Register a patient

MSH	Message Header
EVN	Event Type
PID	Patient Identification
PV1	Patient Visit

Symbol	Usage
|	Field separator
^	Component separator
~	Repetition separator
\	Escape character
&	Subcomponent separator
<CR>	Segment terminator

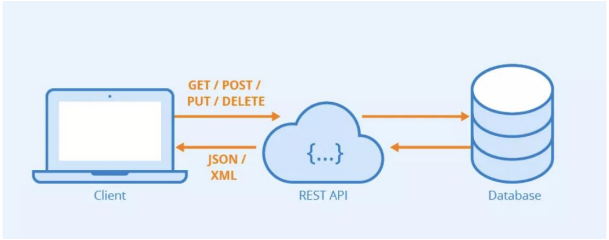


How do you create something like this?

- *public clouds*
- *private clouds*
- *hybrid clouds*

Core Idea: REST

- Representational State Transfer (RESTful) APIs
- Built to copy the web
- Organised around the concept of "Resources"
- All resources have references to other resources, extensions, and a human readable XHTML display
- Augmentation by Messages and Document paradigm also possible
- Open license, a focus on implementation, and a formal maturity process linked to implementation outcome.



Standard REST APIs

FHIR APIs

FHIR Standard

```json
{
  "resourceType": "Bundle",
  "type": "message",
  "entry": [
    {
      "resource": {
        "resourceType": "MessageHeader",
        "eventCoding": {
          "system": "http://hl7.org/fhir/message-events",
          "code": "ADT_A01"
        },
        "destination": [
          {
            "endpoint": "http://localhost:8080/fhir/baseDstu3"
          }
        ],
        "source": {
          "name": "ADT1",
          "software": "GOOD HEALTH HOSPITAL",
          "endpoint": "http://localhost:8080/fhir/baseDstu3"
```

Deep Dive

- **Level 1: Foundation**—The standard's basic framework (**30 resources**). It is divided into Conformance, Terminology, Security, Documents and Other subcategories.
- **Level 2: Base**—Support for implementation and binding to external specifications (**26 resources).** It is divided into Individuals, Entities #1, Entities #2, Workflow and Management subcategories.
- **Level 3: Clinical**—Structural and process elements of real-world health care systems (**39 resources**). It is divided into Summary, Diagnostics, Medications, Care Provision and Request & Response subcategories.
- **Level 4: Financial**—Record-keeping and data exchange (**16 resources**). It is divided into Support, Billing, Payment and General subcategories.
- **Level 5: Specialized**—Providing the ability to reason about health care processes (**35 resources**). It is divided into Public Health & Research, Definitional Artifacts, Evidence-based Medicine, Quality Reporting & Testing and Medication Definition subcategories.

Deep Dive into FHIR Resources

Conformance	Resources describe how a system does or should work	Conformance, StructureDefinition, ValueSet
Infrastructure	Resources defined as part of the API to provide API related services, or basic IT infrastructure	Bundle, List, AuditEvent
Administration	Resources to manage the administrative side of healthcare – who the participants are, where they are or should be, and managing workflow	Patient, Encounter, Appointment, Order / OrderResponse
Clinical	Clinical summaries, record keeping and planning	Observation, Condition, Care Plan, AllergyIntolerance
Financial	Resources that support the financial services associated with the provision of healthcare	Claim, Coverage, ExplanationOfBenefit

Example of Conformance

Due diligence with data: Data Quality Assessments

Conformance

Value Conformance	Value Conformance (Do we have right list of values in “Gender” field ? Do we have correct range of values in “Temp” ? Do we have the right “UOM ?
Schema and Relation Conformance	Is ORU R01 HL7V2 in expected message format ?)

Accuracy

Are data values present ?	Discharge time is missed in data- last 24 hours.
Are data values good ?	Possible duplicate patients. Temp values out of range.Sex values agree with sex specific contexts (pregnancy, prostate cancer) Data values and distributions (including subgroup distributions) agree with trusted reference standards

Data Distribution in source systems

Data distribution/ Source Variations	Counts of unique patients by diagnosis code / procedure code /encounter type is as expected. Distribution of encounters per patient or medications per encounter are as expected. Types of patient population in source #1 vs. source #2.
Training / Serving Skew	If real time data look different from historical data, models will perform differently. Relationship between predictors to outcome may change over time - better treatment plan, new life saving device/procedure/drug and so on.

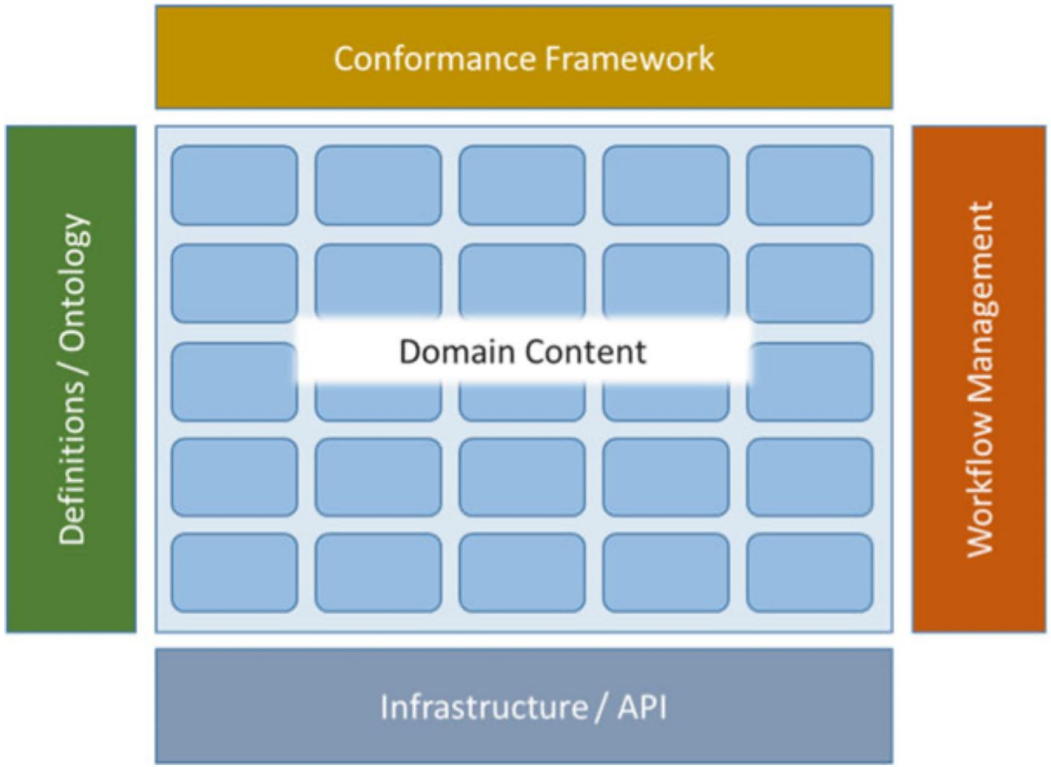
Value Sets & Profiles

Code	Display	Definition
food	Food	Any substance consumed to provide nutritional support for the body.
medication	Medication	Substances administered to achieve a physiological effect.
environment	Environment	Any substances that are encountered in the environment, including any substance not already classified as food, medication, or
biologic	Biologic	A preparation that is synthesized from living organisms or their products, especially a human or animal protein, such as a hormone or antitoxin, that is used as a diagnostic, preventive, or therapeutic agen.Examples of biologic medications include: vaccines; allergenic extracts, which are used for both diagnosis and treatment (for example, allergy shots); gene therapies; cellular therapies. There are

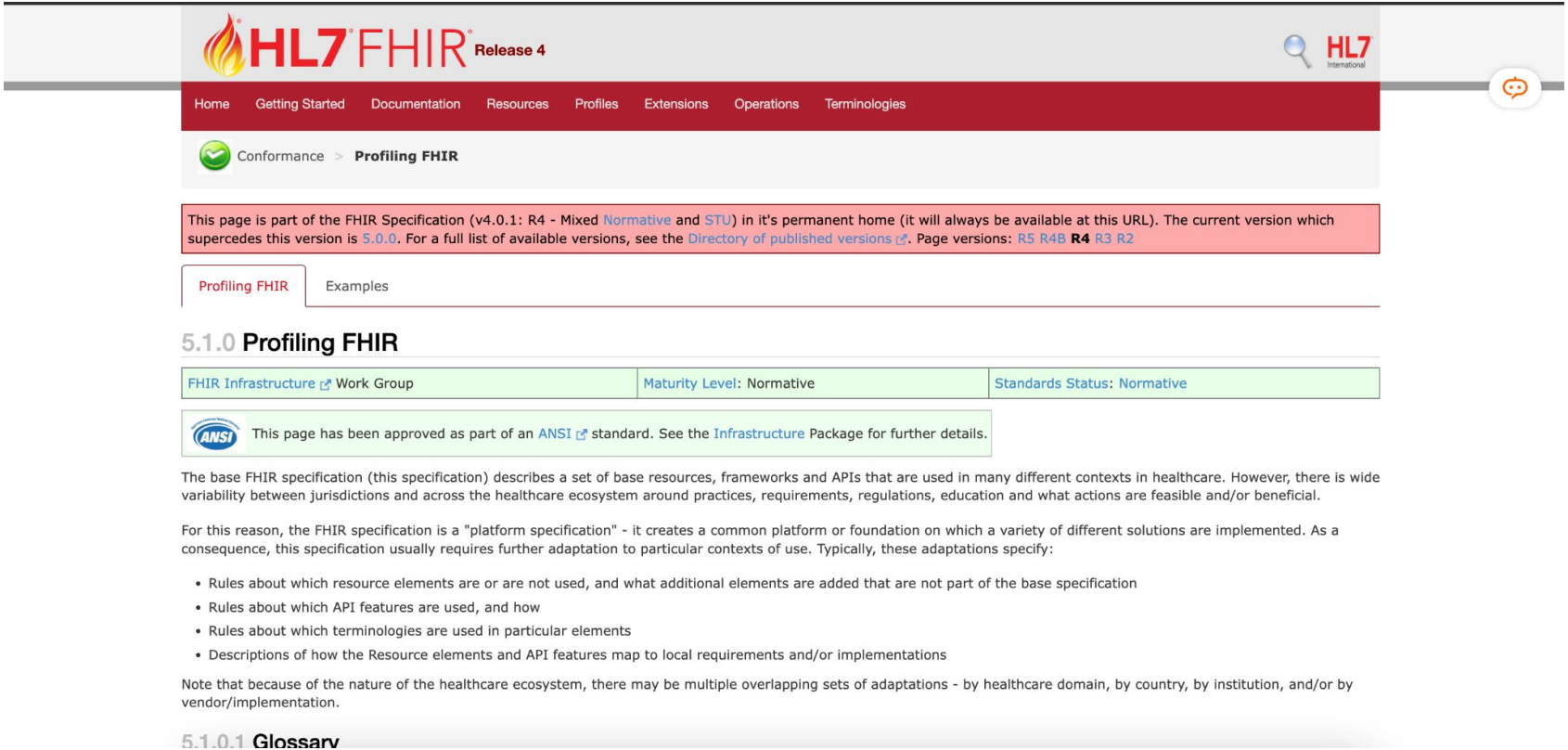

```
{
  "resourceType": "ValueSet",
  "id": "example-gender",
  "status": "active",
  "description": "Example Value Set for Gender",
  "compose": {
    "include": [
      {
        "system": "http://hl7.org/fhir/administrative-gender",
        "concept": [
          { "code": "male", "display": "Male" },
          { "code": "female", "display": "Female" },
          { "code": "other", "display": "Other" },
          { "code": "unknown", "display": "Unknown" }
        ]
      }
    ]
  }
}
```


Note the Difference from Profiles which Provide a set of constraints on a resource for particular **contexts** of use.

FHIR Spec


Conformance Framework
Definitions / Ontology
Domain Content
Workflow Management
Infrastructure / API

Profiling a FHIR Resource



HL7 FHIR Release 4

HL7 International

Home | Getting Started | Documentation | Resources | Profiles | Extensions | Operations | Terminologies

Conformance > **Profiling FHIR**

This page is part of the FHIR Specification (v4.0.1: R4 - Mixed Normative and STU) in it's permanent home (it will always be available at this URL). The current version which supercedes this version is 5.0.0. For a full list of available versions, see the Directory of published versions. Page versions: R5 R4B **R4** R3 R2

Profiling FHIR | Examples

5.1.0 Profiling FHIR

FHIR Infrastructure Work Group	Maturity Level: Normative	Standards Status: Normative

ANSI This page has been approved as part of an ANSI standard. See the Infrastructure Package for further details.

The base FHIR specification (this specification) describes a set of base resources, frameworks and APIs that are used in many different contexts in healthcare. However, there is wide variability between jurisdictions and across the healthcare ecosystem around practices, requirements, regulations, education and what actions are feasible and/or beneficial.

For this reason, the FHIR specification is a "platform specification" - it creates a common platform or foundation on which a variety of different solutions are implemented. As a consequence, this specification usually requires further adaptation to particular contexts of use. Typically, these adaptations specify:

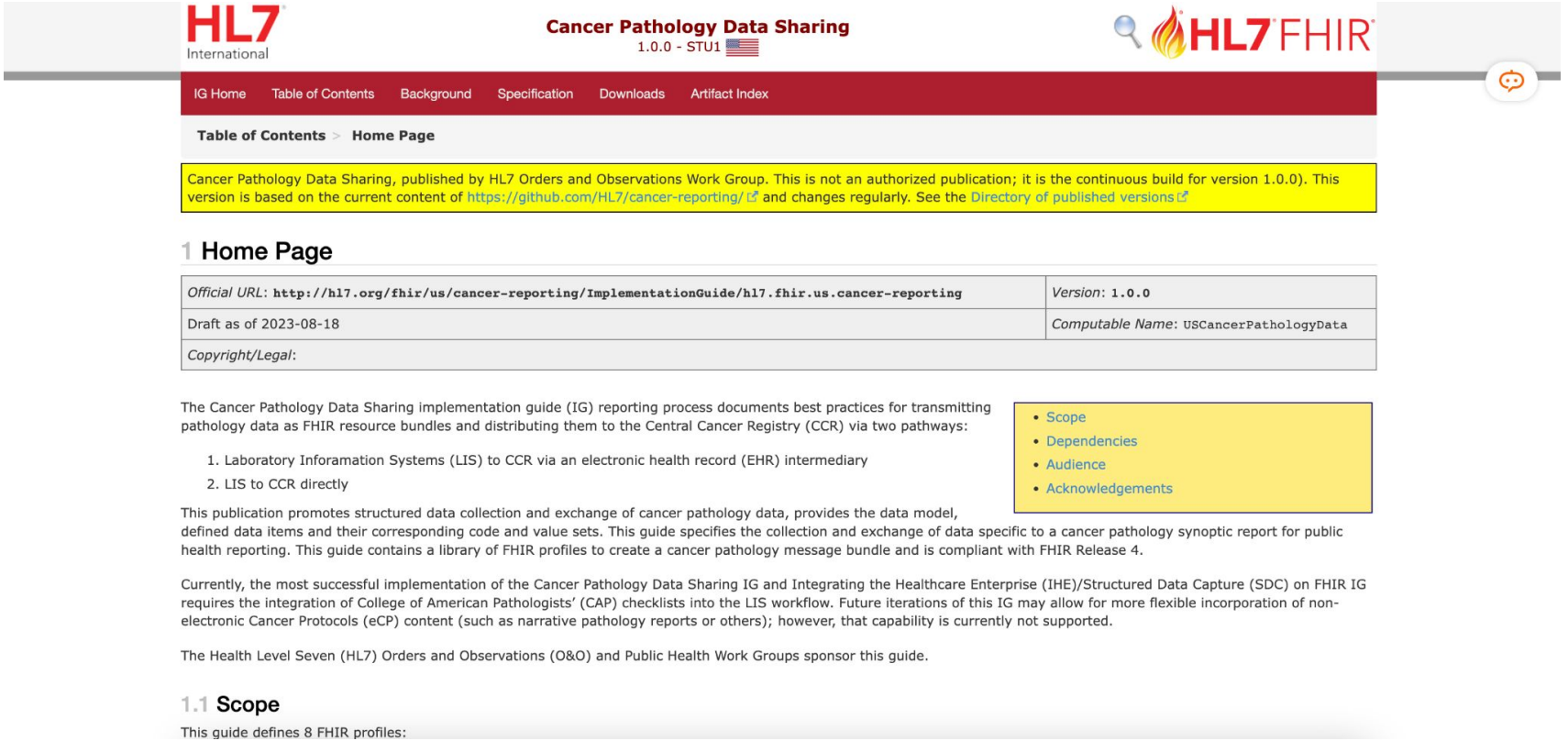
- Rules about which resource elements are or are not used, and what additional elements are added that are not part of the base specification
- Rules about which API features are used, and how
- Rules about which terminologies are used in particular elements
- Descriptions of how the Resource elements and API features map to local requirements and/or implementations

Note that because of the nature of the healthcare ecosystem, there may be multiple overlapping sets of adaptations - by healthcare domain, by country, by institution, and/or by vendor/implementation.

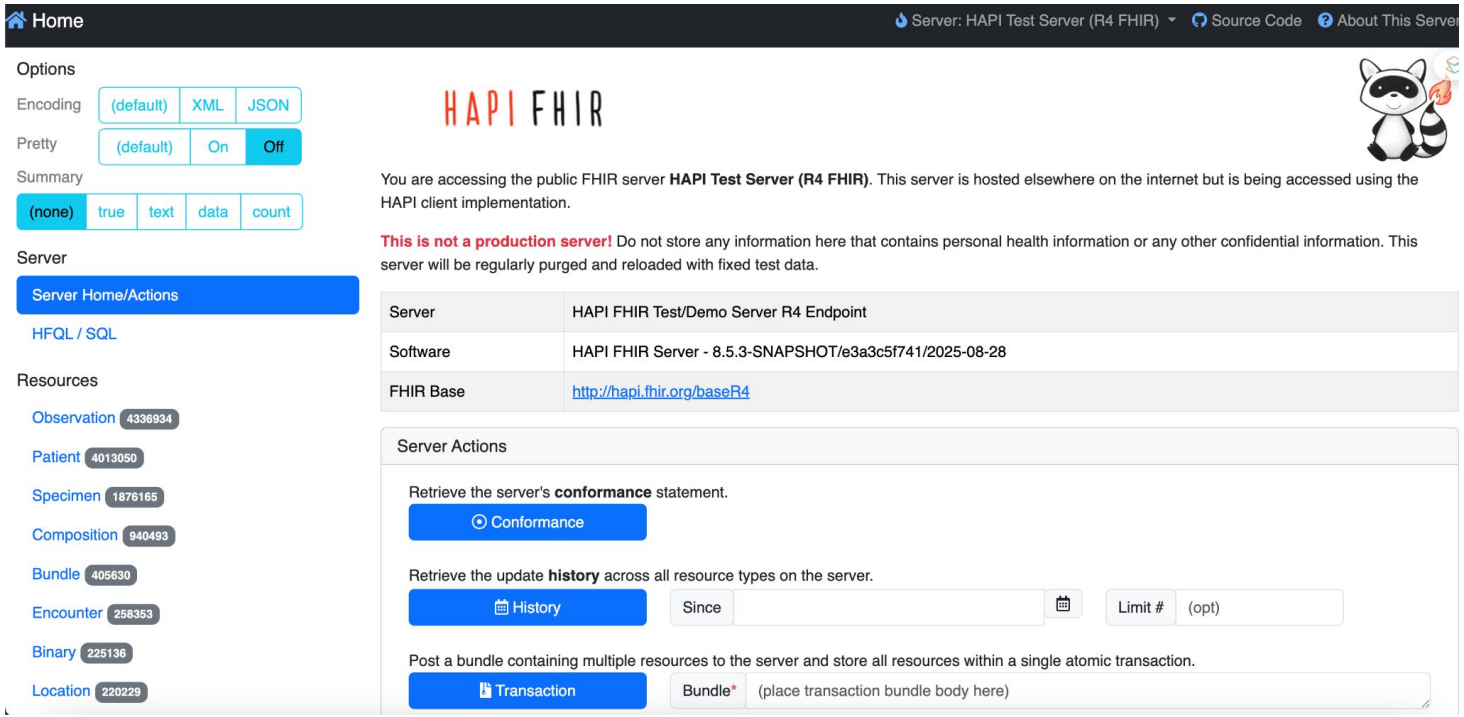
5.1.0.1 Glossary

https://build.fhir.org/ig/HL7/cancer-reporting/

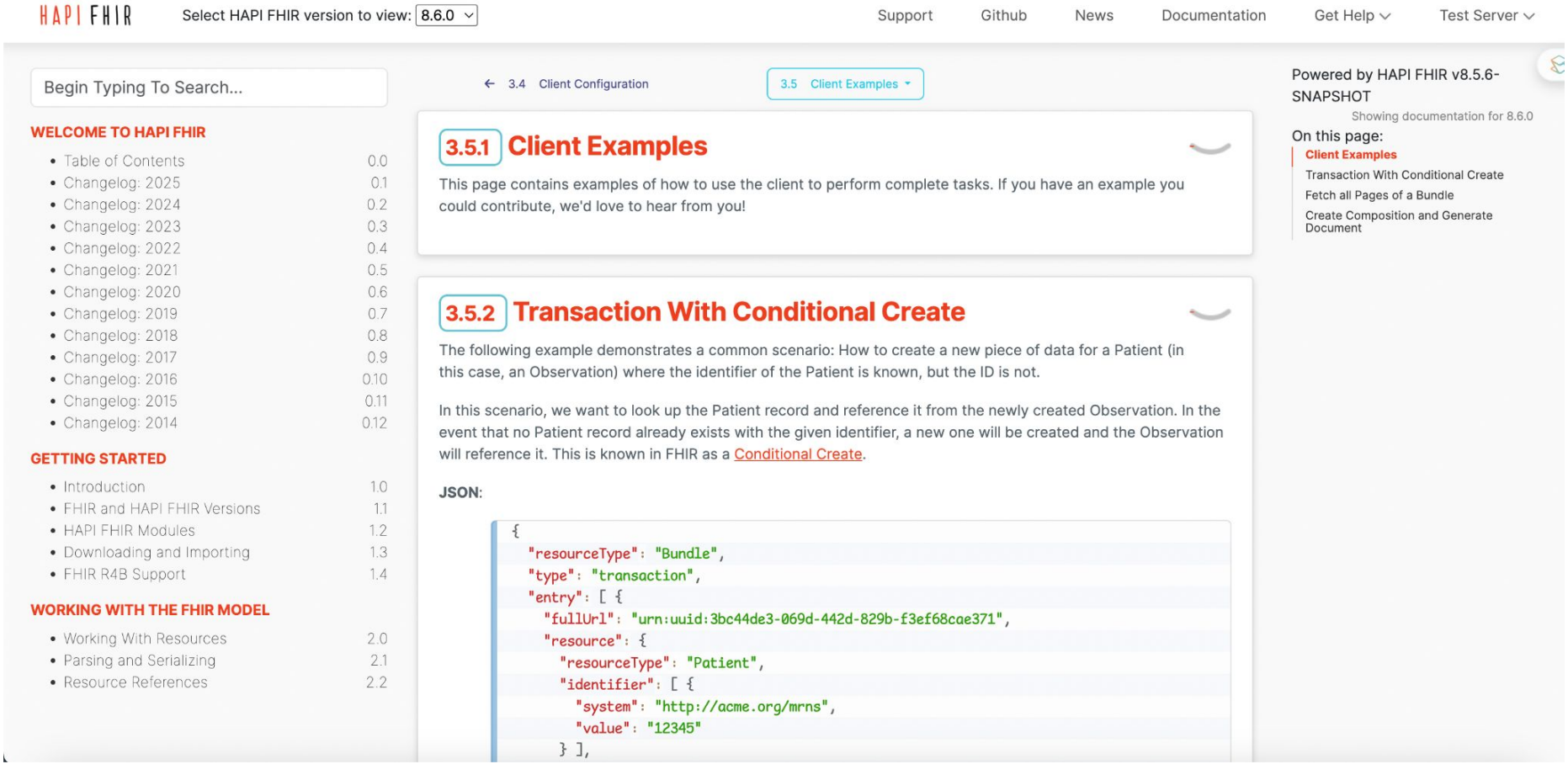
Follow the page link for understanding resources



Openly Available FHIR Servers: HAPI FHIR

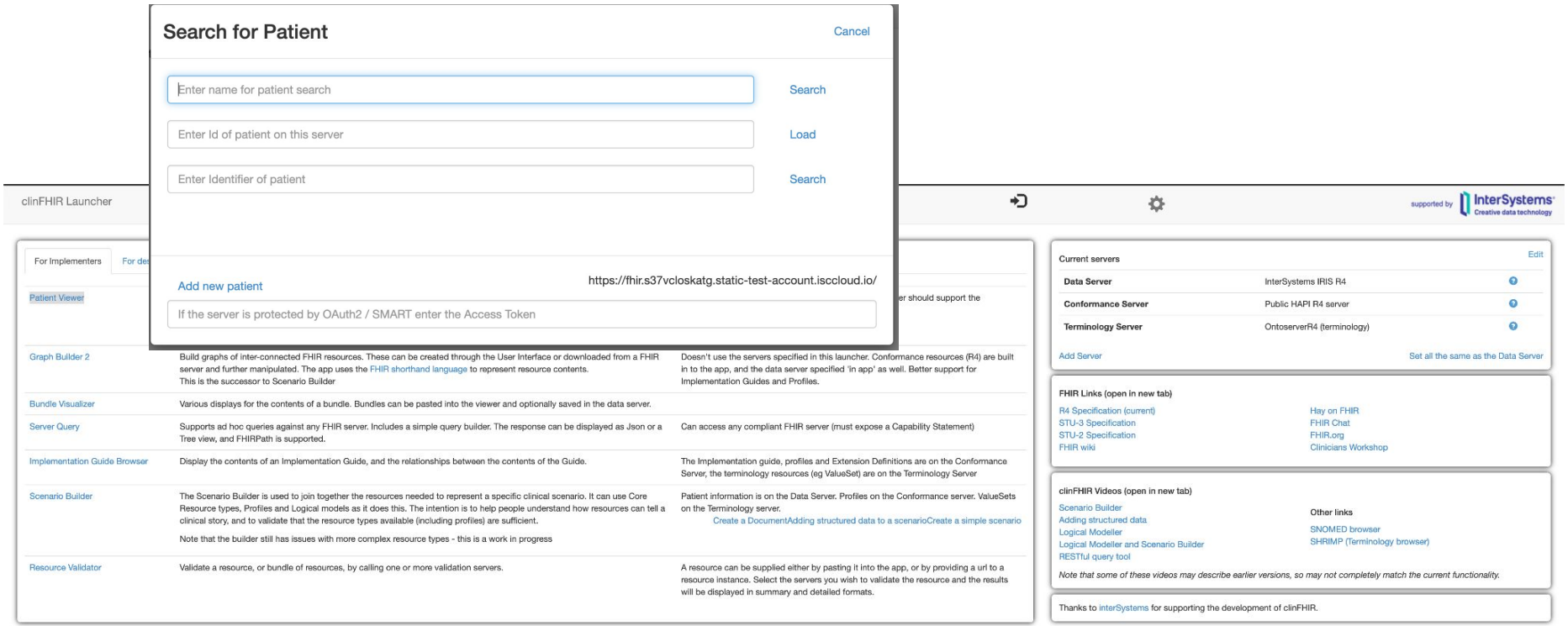


https://hapi.fhir.org/baseR4



https://hapifhir.io/hapi-fhir/docs/client/examples.html

Hands On: Explore ClinFHIR & HAPI FHIR



http://clinfhir.com/

Example: Patient Resource

```
<Patient xmlns="http://hl7.org/fhir">
  <id value="glossy"/>
  <meta>
    <lastUpdated value="2014-11-13T11:41:00+11:00"/>
  </meta>
  <text>
    <status value="generated"/>
    <div xmlns="http://www.w3.org/1999/xhtml">
      <p>Henry Levin the 7th</p>
      <p>MRN: 123456. Male, 24-Sept 1932</p>
    </div>
  </text>
  <extension url="http://example.org/StructureDefinition/trials">
    <valueCode value="renal"/>
  </extension>
  <identifier>
    <use value="usual"/>
    <type>
      <coding>
        <system value="http://hl7.org/fhir/v2/0203"/>
        <code value="MR"/>
      </coding>
    </type>
    <system value="http://www.goodhealth.org/identifiers/mrn"/>
    <value value="123456"/>
  </identifier>
  <active value="true"/>
  <name>
    <family value="Levin"/>
    <given value="Henry"/>
    <suffix value="The 7th"/>
  </name>
  <gender value="male"/>
  <birthDate value="1932-09-24"/>
  <careProvider>
    <reference value="Organization/2"/>
    <display value="Good Health Clinic"/>
  </careProvider>
</Patient>
```

Resource Identity & Metadata

Human Readable Summary

Extension with URL to definition

Standard Data:

- MRN
- Name
- Gender
- Birth Date
- Provider

Summary of the resource

Section	Purpose	Key Elements
Resource Identity & Metadata	Tracks and manages the version and identity of this patient resource.	`id`, `meta.lastUpdated`
Human Readable Summary	Ensures clinicians can read an intelligible summary of the patient's data.	`text`, `div`, `p`
Extension	Adds non-core data while keeping the structure valid.	`extension`, `url`, `valueCode`
Identifier	Holds formal IDs such as MRN.	`identifier`, `system`, `value`
Standard Demographics	Core patient attributes and provider linkage.	`name`, `gender`, `birthDate`, `careProvider`

Example JSON for the Patient Resource

json


```
{
  "resourceType": "Patient",
  "id": "glossy",
  "meta": {
    "lastUpdated": "2014-11-13T11:41:00+11:00"
  },
  "text": {
    "status": "generated",
    "div": "<div xmlns=\"http://www.w3.org/1999/xhtml\"><p>Henry Levin the
  },
  "extension": [
    {
      "url": "http://example.org/StructureDefinition/trials",
      "valueCode": "renal"
    }
  ],
  "identifier": [
    {
```

FHIR Scope of Models: General to Specific

Scope: General Message Definitions to Implementable Message Specifications

- A single domain-wide model (reference model), e.g. HL7 v3/RIM, ISO 13606, FHIR Resource definitions
- Technology-independent specifications constraining the domain wide model, e.g. HL7 v3/RMIMs, CDA Templates, FHIR Profiles and archetypes.
- Implementable message specifications, mappings from technology-independent message specifications into the selected syntax, such as XML or JSON.

Reference Information Model: General Scope

HL7 v3/RIM (Reference Information Model):

- **RIM** is the core, abstract model used by HL7 v3. It provides a standardized, conceptual framework to represent healthcare data across different systems and domains.
- It defines the building blocks (like classes, attributes, and relationships) that are used to create healthcare-related messages, documents, and interactions.
- The RIM is highly abstract and not directly implementable. It serves as the foundation upon which more specific models and standards are built.
- Its purpose is to ensure consistency and a unified approach to handling healthcare information.

Tying the RIM to the Storyboarding

Remember: The RIM contains abstract concepts.

Let’s consider the following example of a patient encounter.

- **Entity**: A person (e.g., the patient or the healthcare provider).
- **Role**: The function of the entity in a particular context (e.g., "Patient" or "Doctor").
- **Act**: An action or event that happens (e.g., "Encounter", "Observation").
- **Participation**: The relationship between a role and an act (e.g., a patient participating in a doctor visit).

Refined Message Information Model: Specific

- **RMIM** is a specialization or refinement of the RIM. It tailors the abstract concepts in the RIM to a particular use case or domain, such as lab results, patient records, or clinical encounters.
- RMIMs are more specific and closer to implementation. They define how data should be structured and exchanged in a given context based on the general principles of the RIM.
- Each RMIM refines the abstract RIM by selecting and constraining the appropriate classes, attributes, and relationships for the specific message or data exchange scenario.

List out the objects at RIM level

Entity (Person)

- Role: Patient

- Role: Healthcare Provider (Doctor)

Act (Encounter)

- Participation: Patient (participates in Encounter)

- Participation: Doctor (participates in Encounter)

List out the details at RMIM level

EncounterMessage (Message Header)

- Act: Encounter (type: Consultation)
  - Participation: Patient (John Doe)
  - Participation: Doctor (Dr. Smith)
  - Observation: Blood Pressure (120/80 mmHg)

Python code stub for RIM

```
# HL7 v3 RIM Abstract Classes

class Entity:

    def __init__(self, name):

        self.name = name
```

```
class Role:
    def __init__(self, entity, role_type):
        self.entity = entity
        self.role_type = role_type
class Act:
    def __init__(self, act_type):
        self.act_type = act_type
        self.participations = []
```

RMIM

```
class EncounterMessage:

    def __init__(self, encounter_type):

        self.encounter = Act(encounter_type)

        self.observations = []
```

RMIM

```
def add_participant(self, entity_name, role_type):
        entity = Entity(entity_name)
        role = Role(entity, role_type)
        participation = Participation(role, self.encounter)
        self.encounter.add_participation(participation)
```

India on FHIR

MAY 23, 2022 • 8 MIN READ

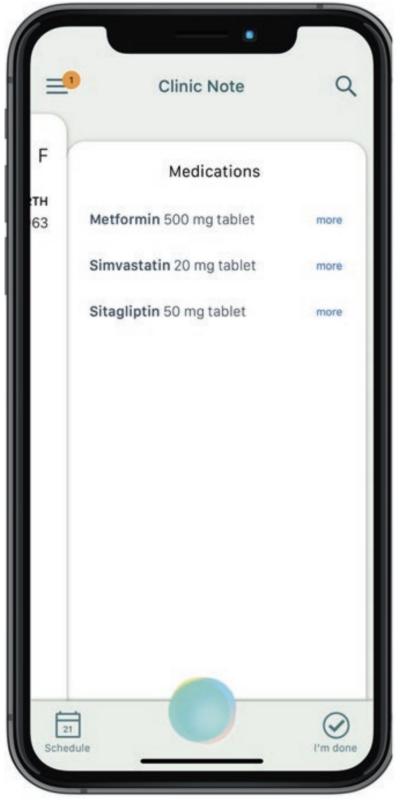
Ayushman Bharat Digital Mission: Ushering in the UPI moment of healthcare

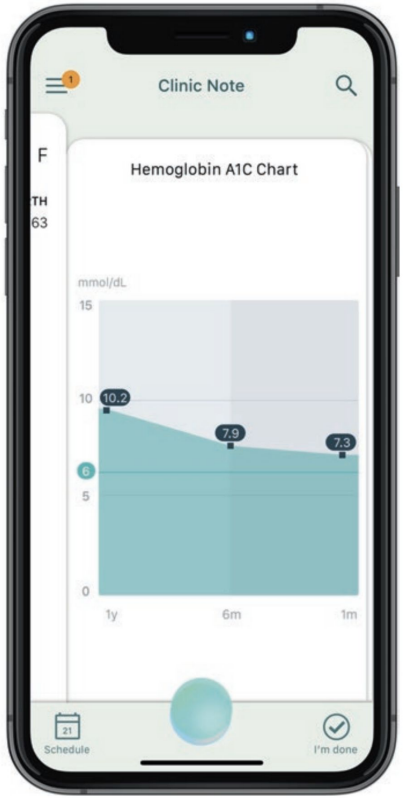
AYUSHMAN BHARAT

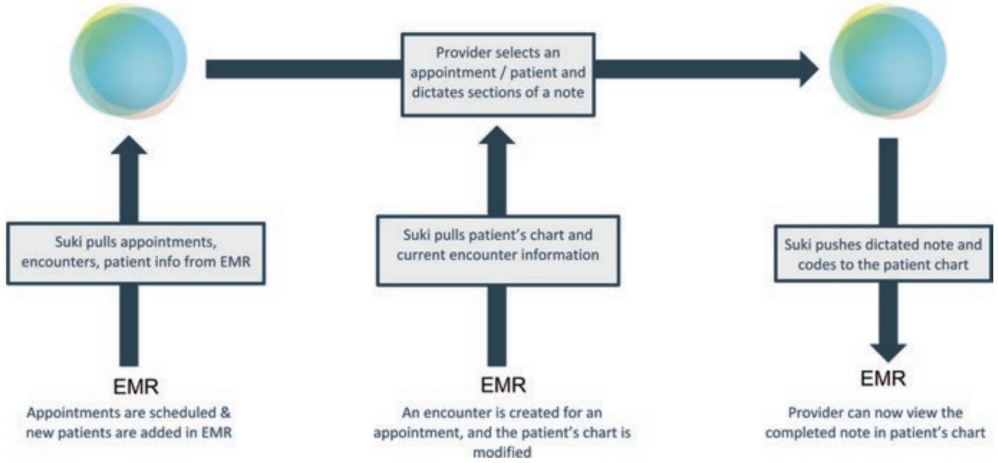
DIGITAL MISSION

Building digital health ecosystem+

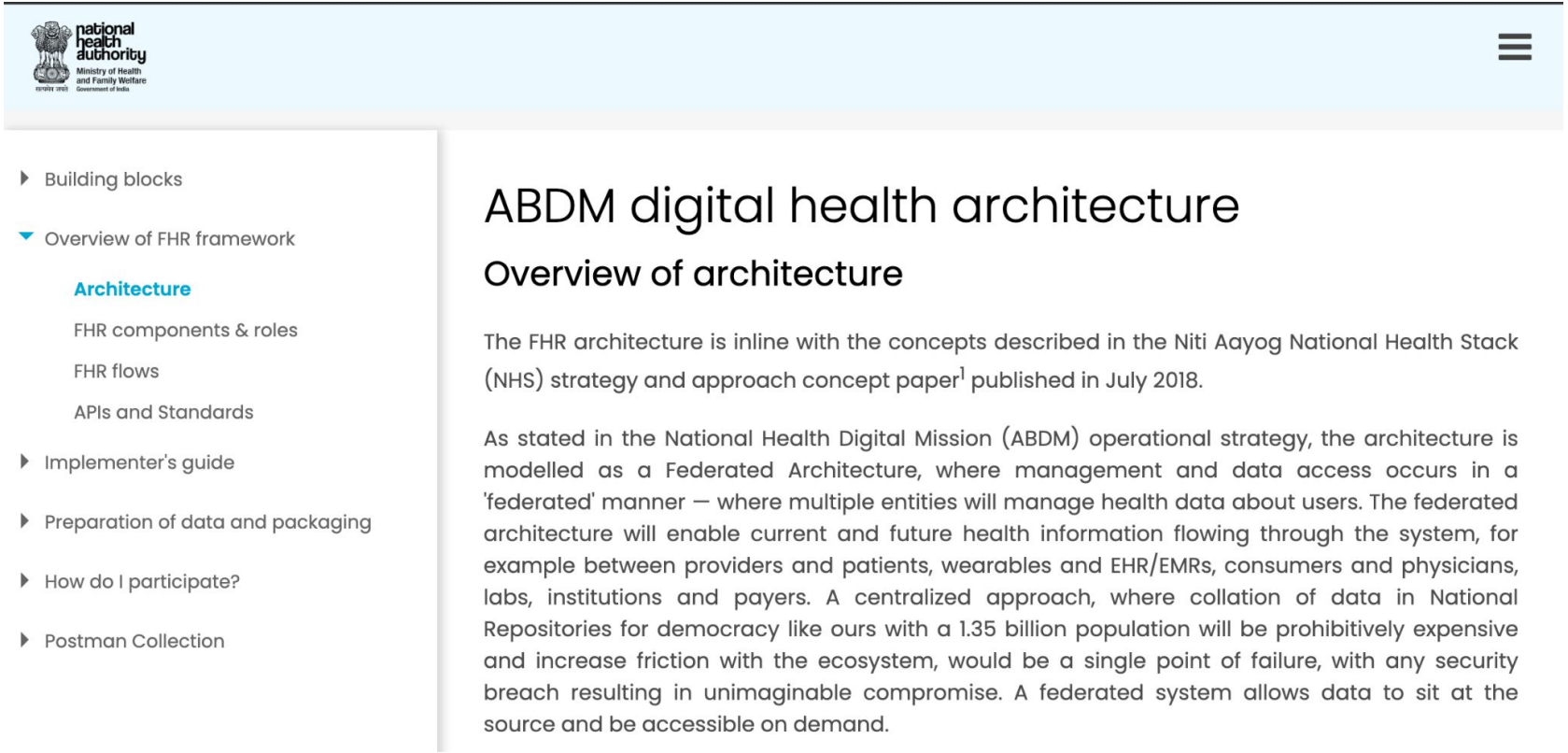
Suki, show me the medications of Mr. Sinha



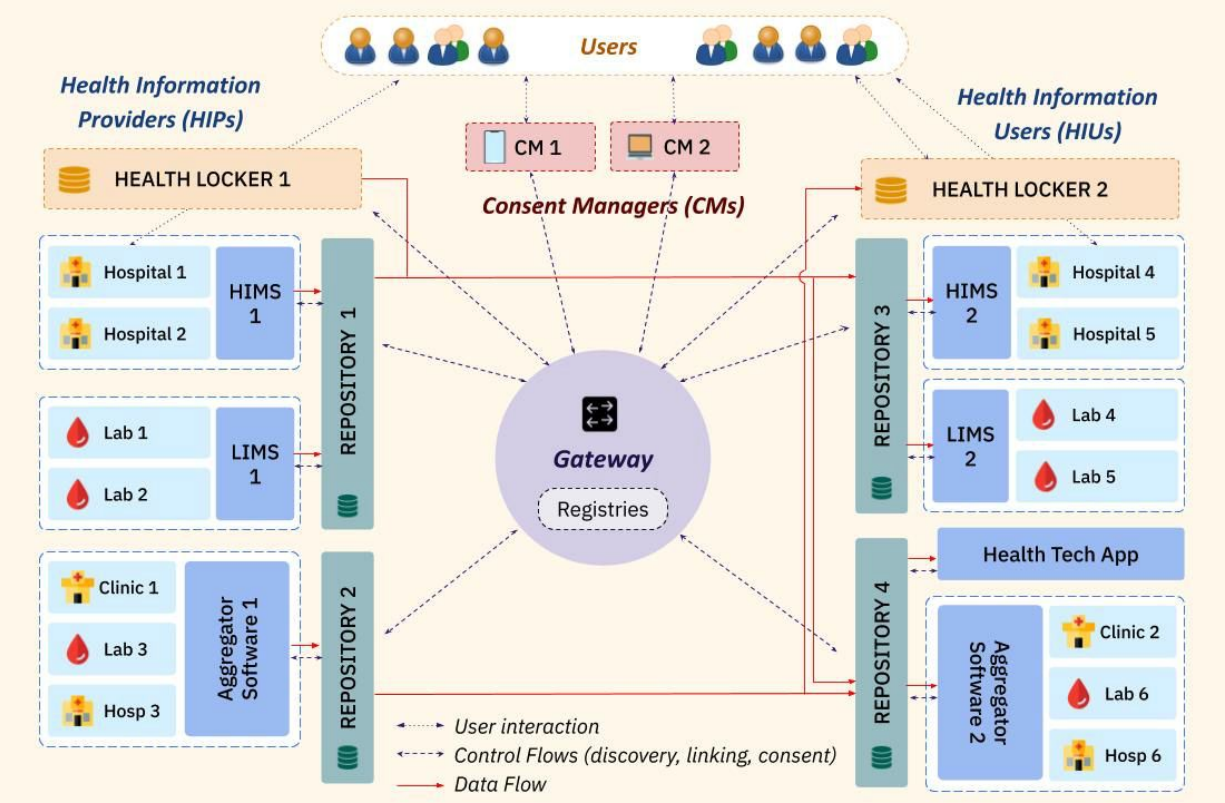




India's FHIR Stack (ABDM)



India's FHIR Stack (ABDM)



FHIR Implementation Guide for ABDM CI Build v2.0.1

Home | Profiles | Terminology | Examples | Downloads

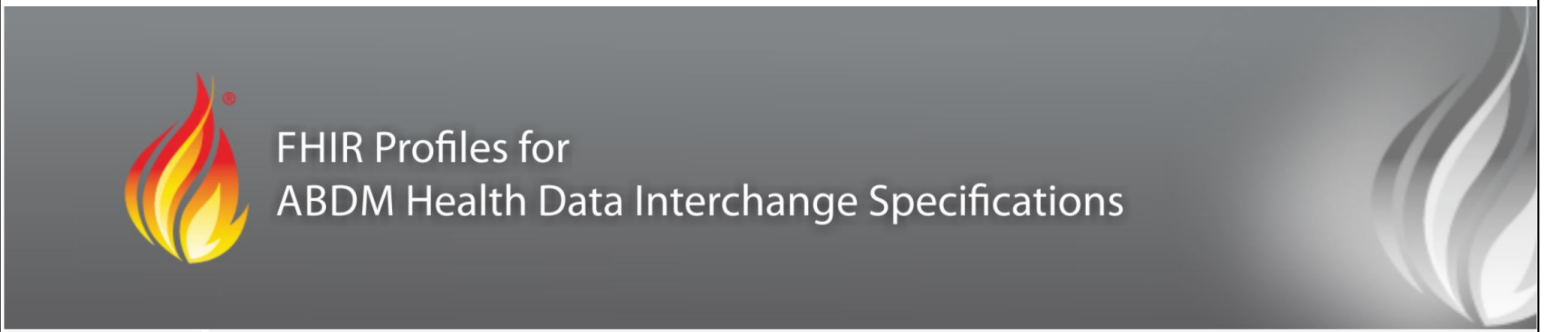


Table of Contents

This Implementation guide is published and maintained by NRCeS for NHA.
This version is based on the ABDM Health Data Interchange Specifications 1.0 and updated periodically.

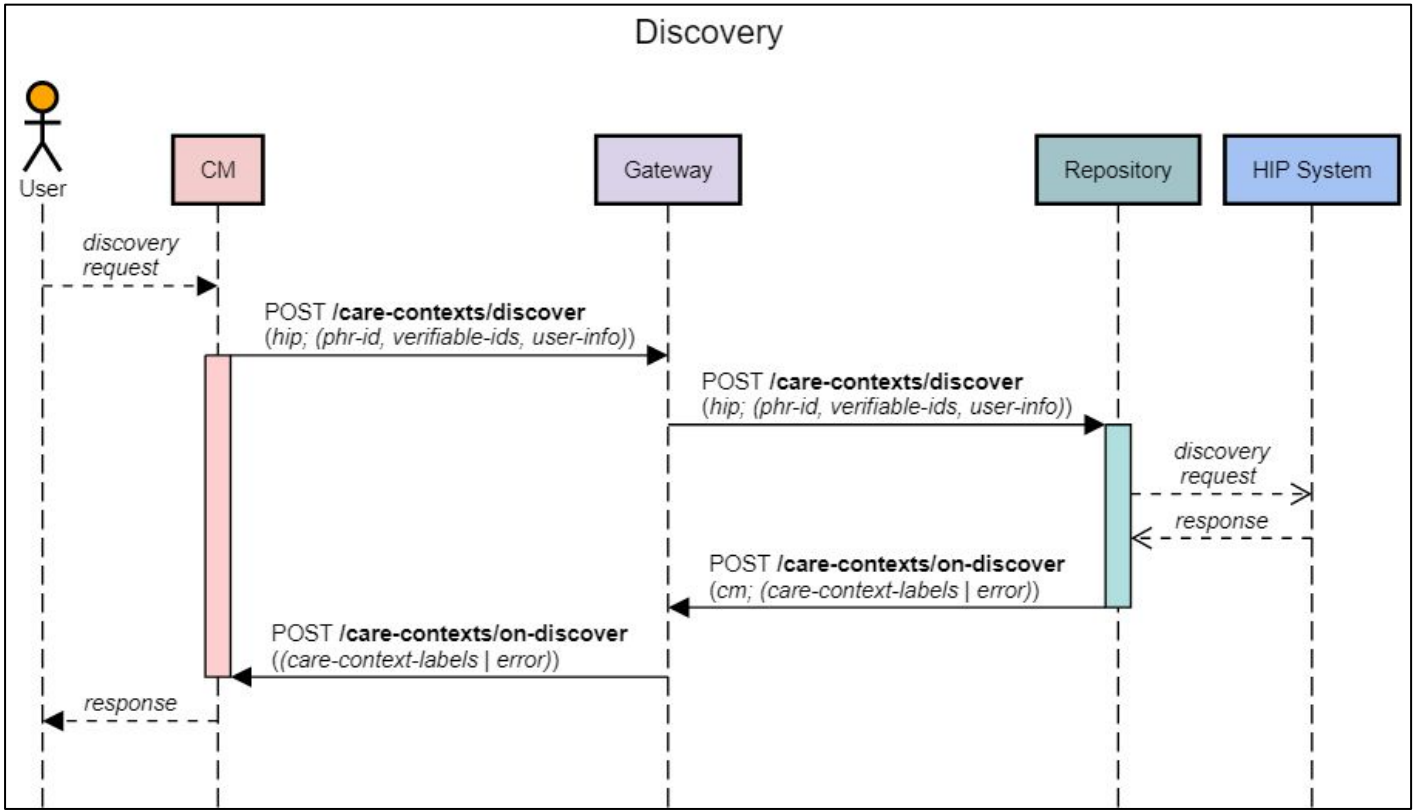
Narrative Content | Detailed Descriptions | Mappings | XML | JSON | Turtle

Definitions for the StructureDefinition-PrescriptionRecord Profile.

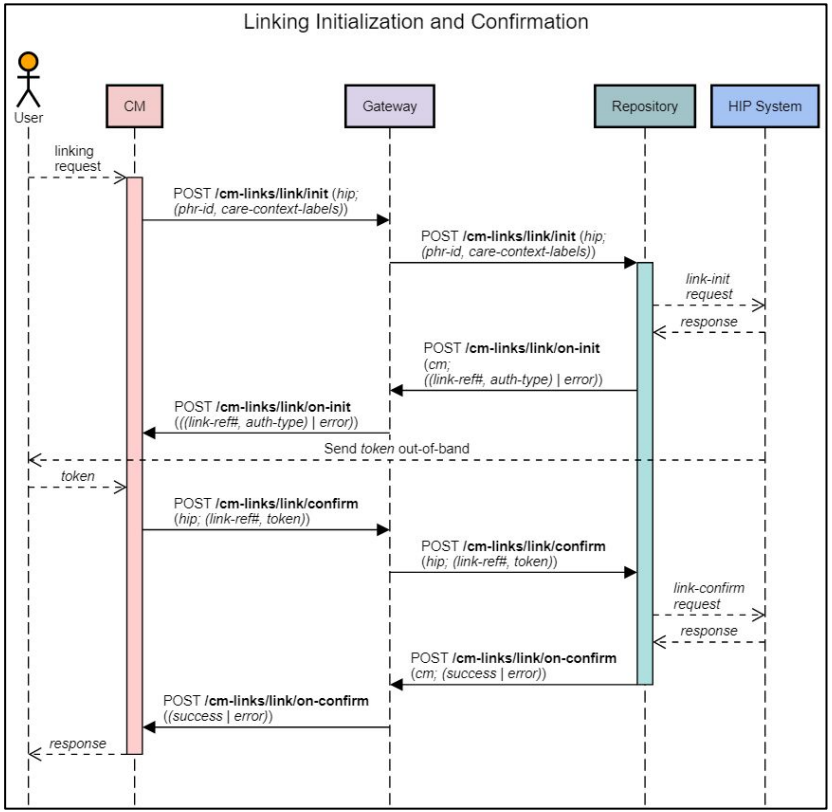
1. Composition

Definition	A set of healthcare-related information that is assembled together into a single logical package that provides a single coherent statement of meaning, establishes its own context and that has clinical attestation with regard to who is making the statement. A Composition defines the structure and narrative content necessary for a document. However, a Composition alone does not constitute a document. Rather, the Composition must be the first entry in a Bundle where Bundle.type=document, and any other resources referenced from Composition must be included as subsequent entries in the Bundle (for example Patient, Practitioner, Encounter, etc.). A set of healthcare-related information that is assembled together into a Composition to represent a physician's order for the preparation and administration of a drug or device for a patient. A Composition defines the structure, it does not actually contain the content: rather the full content of a document (for example Patient, Practitioner, Organization, MedicationRequest, etc.) is contained in a Bundle, of which the Composition is the first resource contained.

Discovery of Patient Information



Linking to Hospital (HIP)



Health ID and Consent Management Framework

Health data consent manager (HDCM)

HDCM plays the role of fiduciary or trustee with which a patient signs up to begin with. The HDCM does the following:

- Helps to create or discover existing ABDM ABHA Number
- Manages patient linkages to providers
- Manages consent for access to health information
- Helps discover patient information
- Monitors information exchange between HIP and HIU

All the above are done via a Patient App. In future, there will be other channels for patients to manage their health data.

Health information gateway

Gateway is the hub that mediates and connects Consent Manager(s), Health Repository Providers and HIUs in the network. Its primary job is to allow for discovery, routing in the network. The gateway does the following:

- Connects and validates the HDCMs and health repositories (servicing HIUs and HIPs) to the network.
- Enables routing of information.
- Authenticates connected systems within the FHR Framework (provides a signed authentication token for

FHR framework including the gateway communicates via asynchronous APIs over HTTPs channel.

Registries

There are various National level Registries that are integrated with the network.

- Health Facility registry (HFR)
- Doctor or practitioner registry (DigiDoctor)
- HDCM and Health Repository Provider (HPR) Registry

The HDCM and HRP registries are currently maintained by the ABDM Gateway.

Health repository

A health repository is the connector or bridge through which any HIU or HIP can connect to the network. The health repository allows HIPs and HIUs to access patient data for a specific period of time. The sandbox environment provides a basic HIU system, representing a doctor's interface. The sandbox environment also provides a mock HIP system using which you can test linkages and access to health information from multiple sources.

https://sandbox.abdm.gov.in/docs/components_roles

Health ID and Consent Management Framework

Registering as a patient using the Patient App

The following sections explain how a patient can register via consent manager app. Once you've registered as a patient, you will be able to search hospitals and choose to link your patient care contexts for the selected one. This will enable access to medical records for a HIU or for the patient herself.

Mobile number verification

To register via the patient app, the first step is to register using a digitally verifiable identifier. As of now, Aadhaar and mobile numbers are such identifiers. In future, more digital identifiers would be supported.

Perform the following tasks to begin your registration process on the Consent Manager app:

1. Install the consent manager application on your phone.
   Download .apk file .
2. Open the Consent Manager app and click on the **Register** button to register as a patient.
3. You will be asked to enter your mobile phone number, in order to verify your identity. Make sure that you enter the mobile number which you generally provide at the hospitals that you visit.
4. Enter your mobile number. Take care to enter valid phone number.
5. Click the **Verify** button to authenticate your mobile number.
6. You will receive an SMS from the ABDM Consent Manager, along with an OTP (One Time Password).
7. Enter the OTP in the Consent Manager app.
8. If your OTP is validated, you will be directed to a Registration screen. If your OTP is not validated, you will be prompted to enter a valid OTP

https://sandbox.abdm.gov.in/docs/flows

HIP services

The following responsibilities are expected to be carried out by HIP services in the FHR Framework context:

- Ability to discover and link patient's care contexts within an organization's system.
- Allow for consented means of exchange of patient's health information in a machine readable format (FHIR), conforming to standards setup by ABDM.
- Provide a secure and safe means of data transfer from organization-specific HIS (Health Information System) instance to a validated and consented requester HIU, through the ABDM Gateway.

HIU services

The following capabilities are expected of HIU services in the FHR context:

- Ability to search for and identify a patient using her ABHA Number. HIU systems can search for patients linked within the ABDM Gateway network, and across diverse Gateway networks in future.
- Ability to request and receive patient data in a safe and secure manner, manage data lifecycle, and enable secure data storage and access.

Health locker services

Health locker provides a personal digital storage for users/patients. The following capabilities are expected of Health locker services in the FHR context:

- Sign up users/patients in their system.
- Allow users to upload their health documents to their locker.
- Ability to fetch users health documents from the HIPs based on patient consent.
- Ability to Provide Health Documents, both self uploaded and fetched from HIPs, to a valid requeste
- Allow user/patient access to their health documents (through their locker apps or other channels
- Provide secure means for health document access and storage.

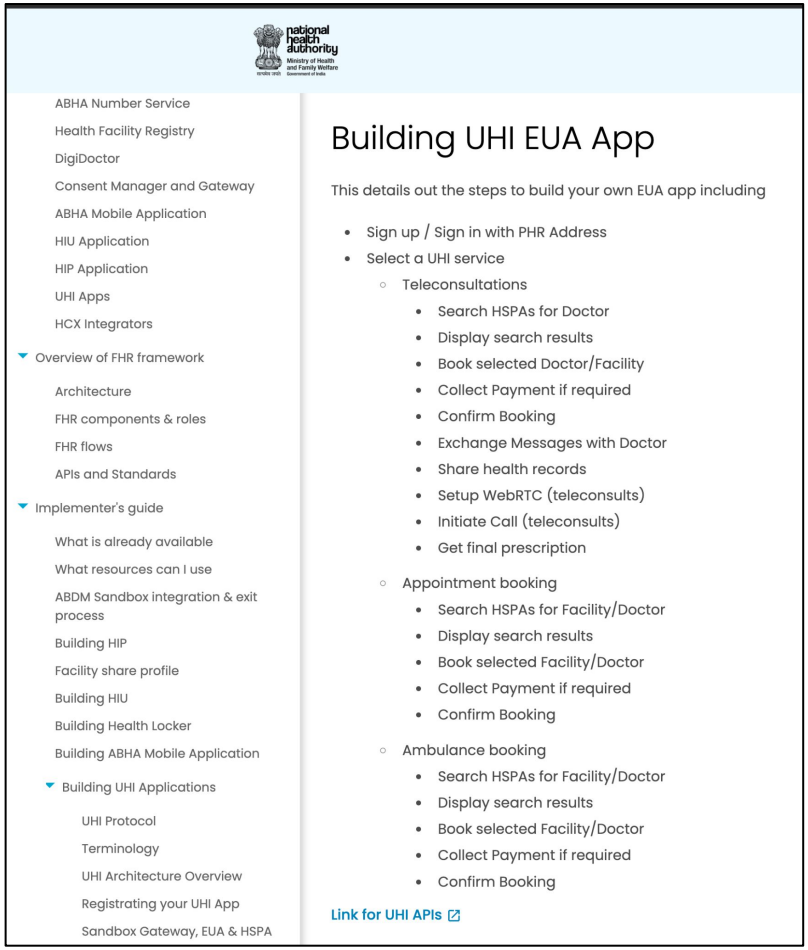
What is a Patient App?

While building and testing your health repository in integration with the sandbox's network components, you'll need to test patient flows as well. For example:

- Signup of patient with Consent Manager (CM)
- Linking patient's CM account with HIP's patient reference and health care contexts
- Granting or revoking consents

You can do all of the above using APIs as well, but the easiest way would be to use the reference patient Android App. Download .apk file .

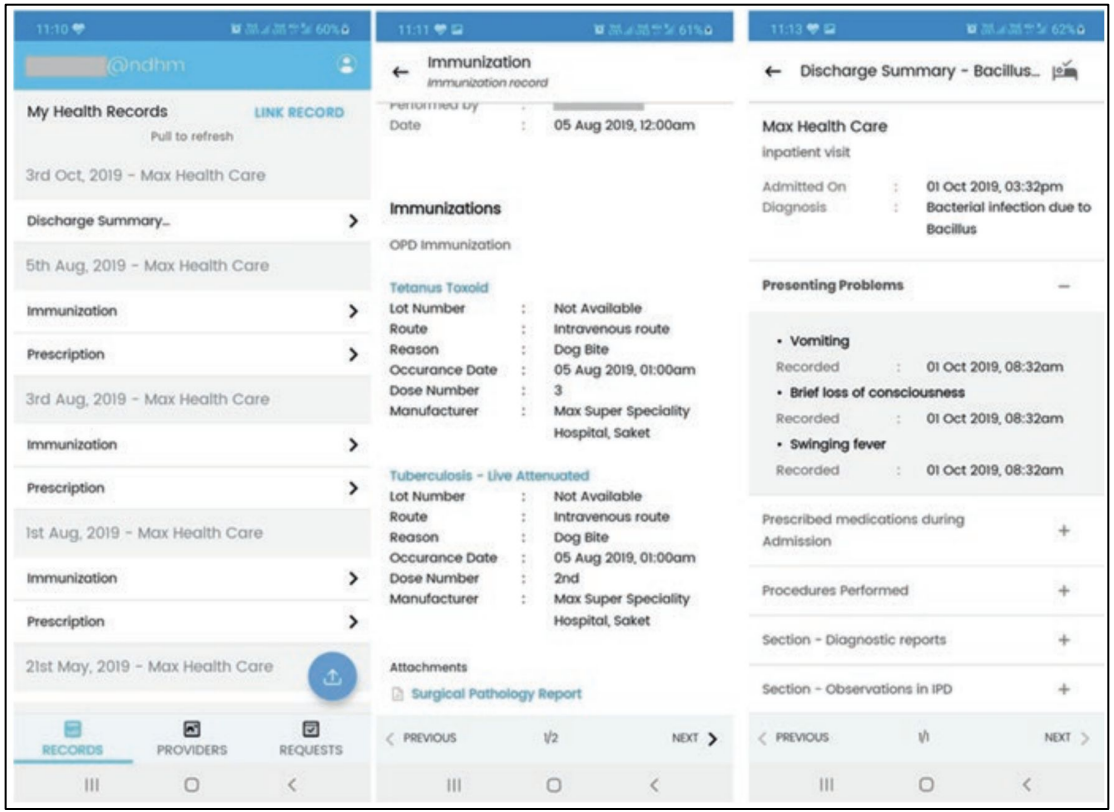
https://sandbox.abdm.gov.in/docs/components_roles



https://sandbox.abdm.gov.in/docs/uhi_eua

Example Apps

Citizen/Patient Services
Single, Secure Health id to all citizens
Personal Health Record
Singel (National) Health Portal
App Store
Specialized Services for Remote Areas/ Disadvantaged Groups
NDHM Call Centre
Digital Referrals & Consultations
Online Appointments
e-Prescription Service
Digital Child Health
National “Opt-out” (for privacy)
Services by / for Healthcare Providers/ Professionals
Summary Care Record
Open Platform to access Emergency Services
Technology for Practitioner (GP) Transformation
Digital Referrals, Case Transfers
Clinical Decision Support (CDS)
Digital Pharmacy & pharmacy Supply Chain
Hospital Digitization (HIS)
Digital Diagnostics
Technical Services
Architecture & Interoperability
Health Information Exchange
Standards
Health Network
Data & Cyber Security
Information Governance



Data encryption and decryption as requester HIU

The following abbreviations are used in this section:

- ECDH: Elliptic-curve Diffie–Hellman Key Exchange
- AES-GCM: Advanced Encryption Standard-Galois/Counter Mode
- DHPK: Elliptic-curve Diffie–Hellman public key
- DHSK: Elliptic-curve Diffie–Hellman secret/private key
- P and U is annotation for system
- DHK(U,P): Elliptic-curve Diffie–Hellman Key
- Rand: Random String

Information shared as part of the data flow will be secured using an encryption mechanism that ensures perfect forwa secrecy. This means that even if any of the key materials stored at HIPs, HIUs or HDCM clients (either long-term private keys session keys) are compromised, it would not be possible to decipher data that was previously exchanged. The encryptic mechanism uses Elliptic-curve Diffie–Hellman Key Exchange (ECDH), which is used in many Internet protocols such as SS and TLS for establishing shared secret keys between remote parties.

Data encryption for HDCM client

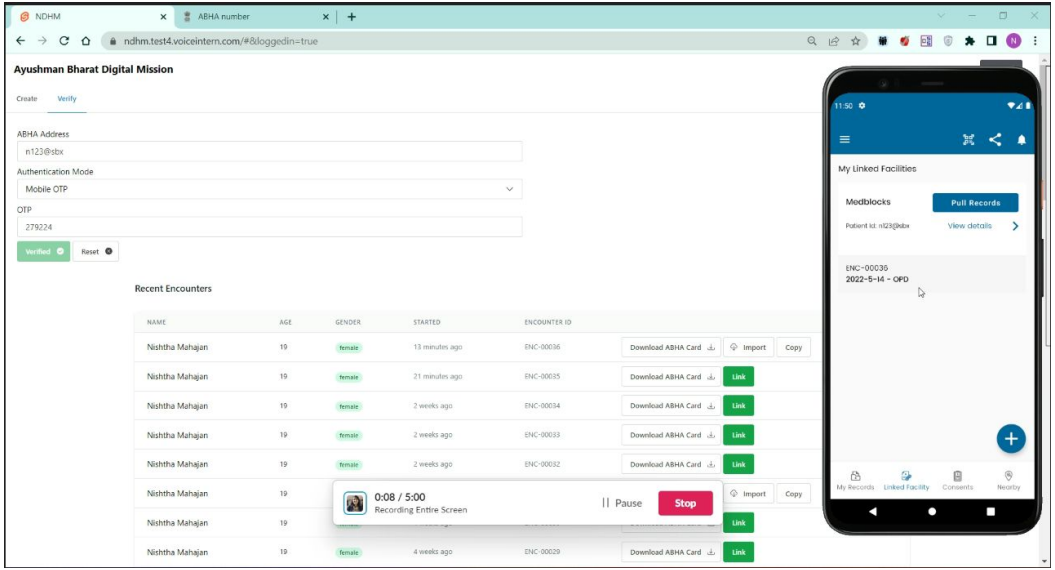
The following points detail the process behind data encryption for HDCM client:

1. When creating a data request, the HIU does the following:
   a. Creates a set of Elliptic-curve Diffie–Hellman (ECDH) parameters
   b. Generates a **ECDH key pair (dhsk(U) , dhpk(U))** (which is a short-term public-private key pair)
   c. Generates a **32-byte random value**, rand(U) which is also called **nonce**.
2. The HIU sends these values to HDCM, along with the data request via a digitally-signed API call.
3. HDCM forwards the request to the HIP, again via a digitally-signed API call.
4. HIP checks whether the consent artefact is valid, and whether the data being requested is in keeping with the terms of the artefact. If the artefact is valid, the HIP does the following:
   - Generates a fresh ECDH public-private key pair in the same group as specified by the HIU **((dhsk(P), dhpk(P))**

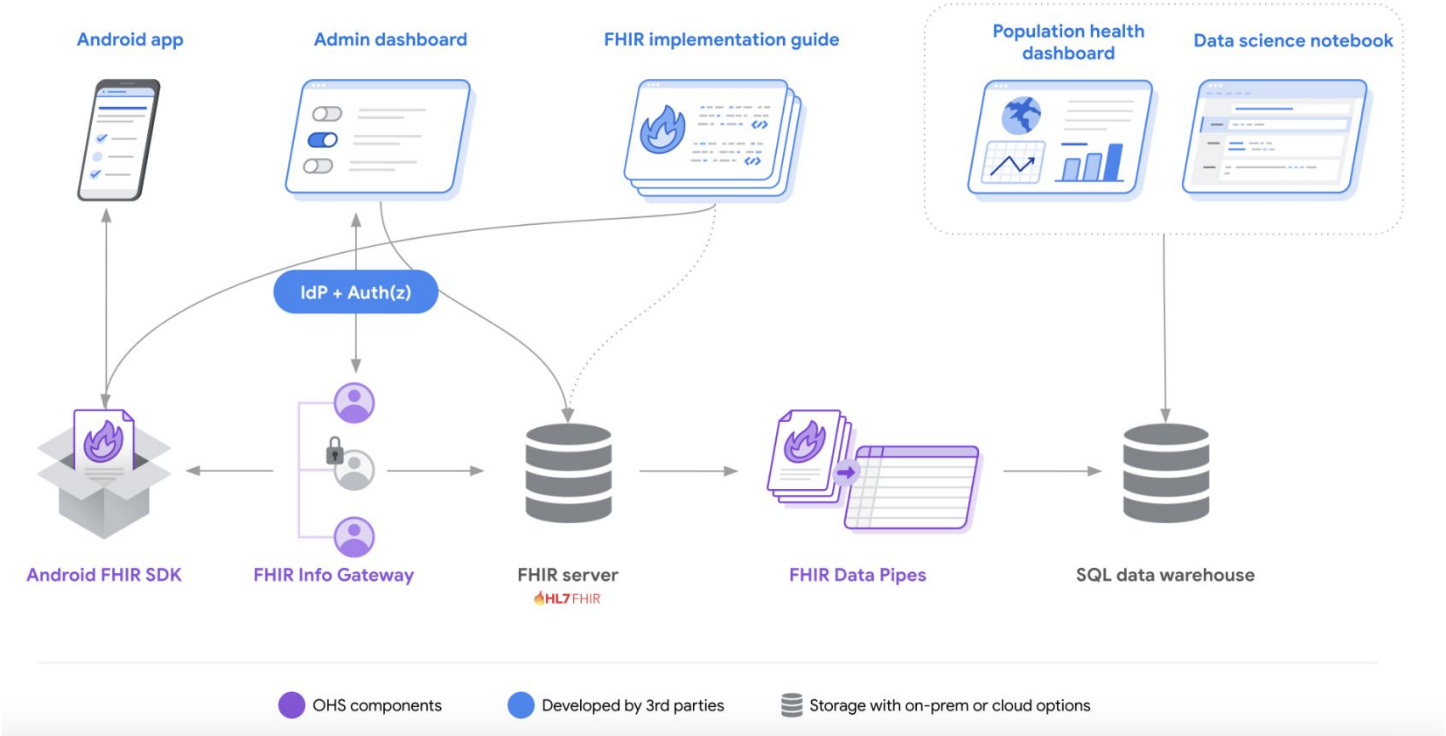
https://medblocks.org/abdm-for-the-ap-government-a-honest-review/

Health ID


Suresh
ABHA Number: XXXXX
ABHA Address: XXXXX
Date of Birth: XXXXX
Gender: XXXXX
Mobile: XXXXX


NDHM
ABHA number
ndhm.test4.voiceintern.com/#&loggedin=true
Ayushman Bharat Digital Mission
Create
Verify
ABHA Address
n123@sbx
Authentication Mode
Mobile OTP
OTP
279224
Verified
Reset
Recent Encounters
NAME
AGE
GENDER
STARTED
ENCOUNTER ID
Nishtha Mahajan
Download ABHA Card
Import
Copy
Link
0:08 / 5:00
Recording Entire Screen
Pause
Stop
My Linked Facilities
Medblocks
Pull Records
View details
ENC-00035
2022-5-14 - OPD

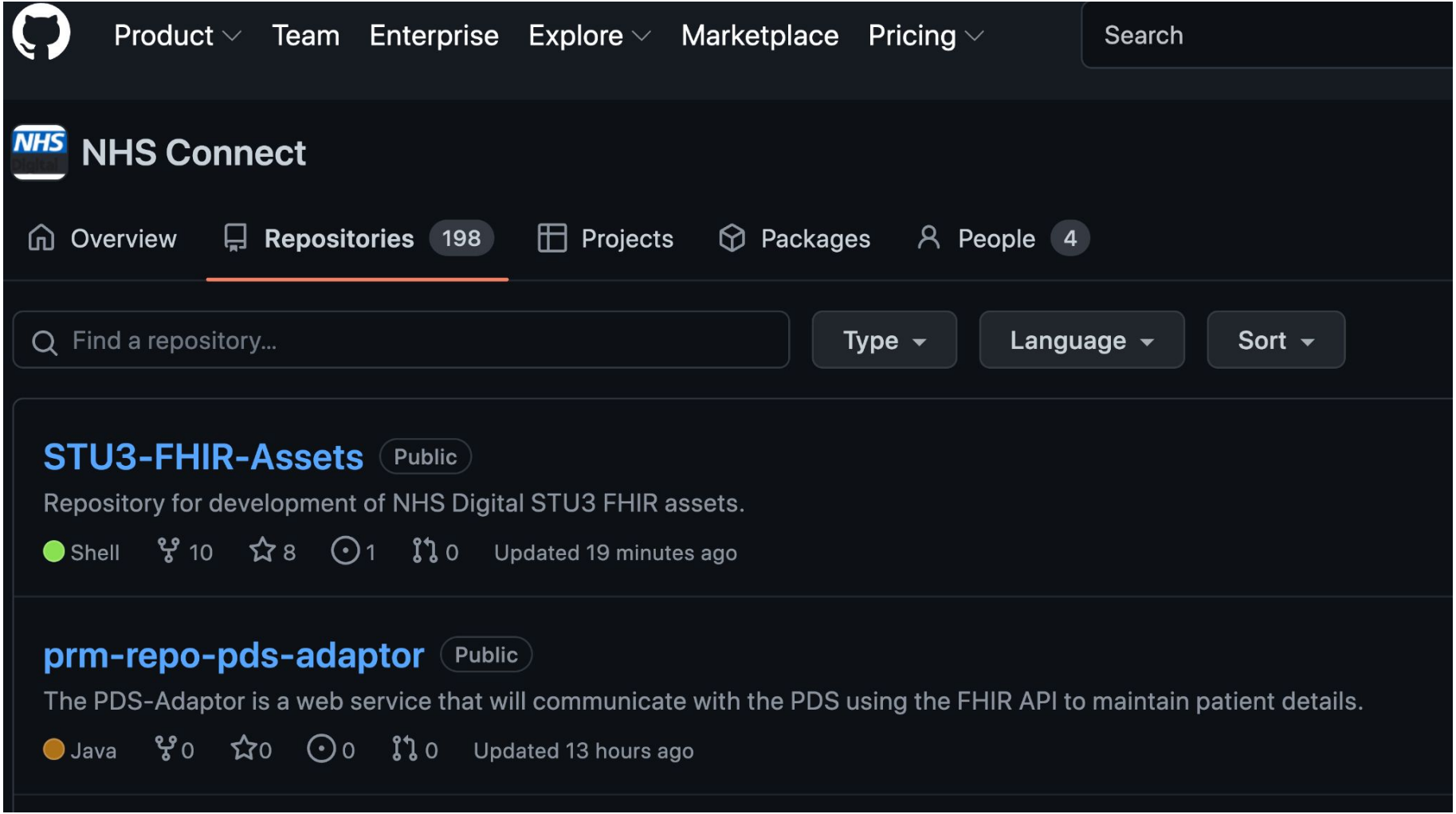
Google on FHIR: Open OHS End to End FHIR

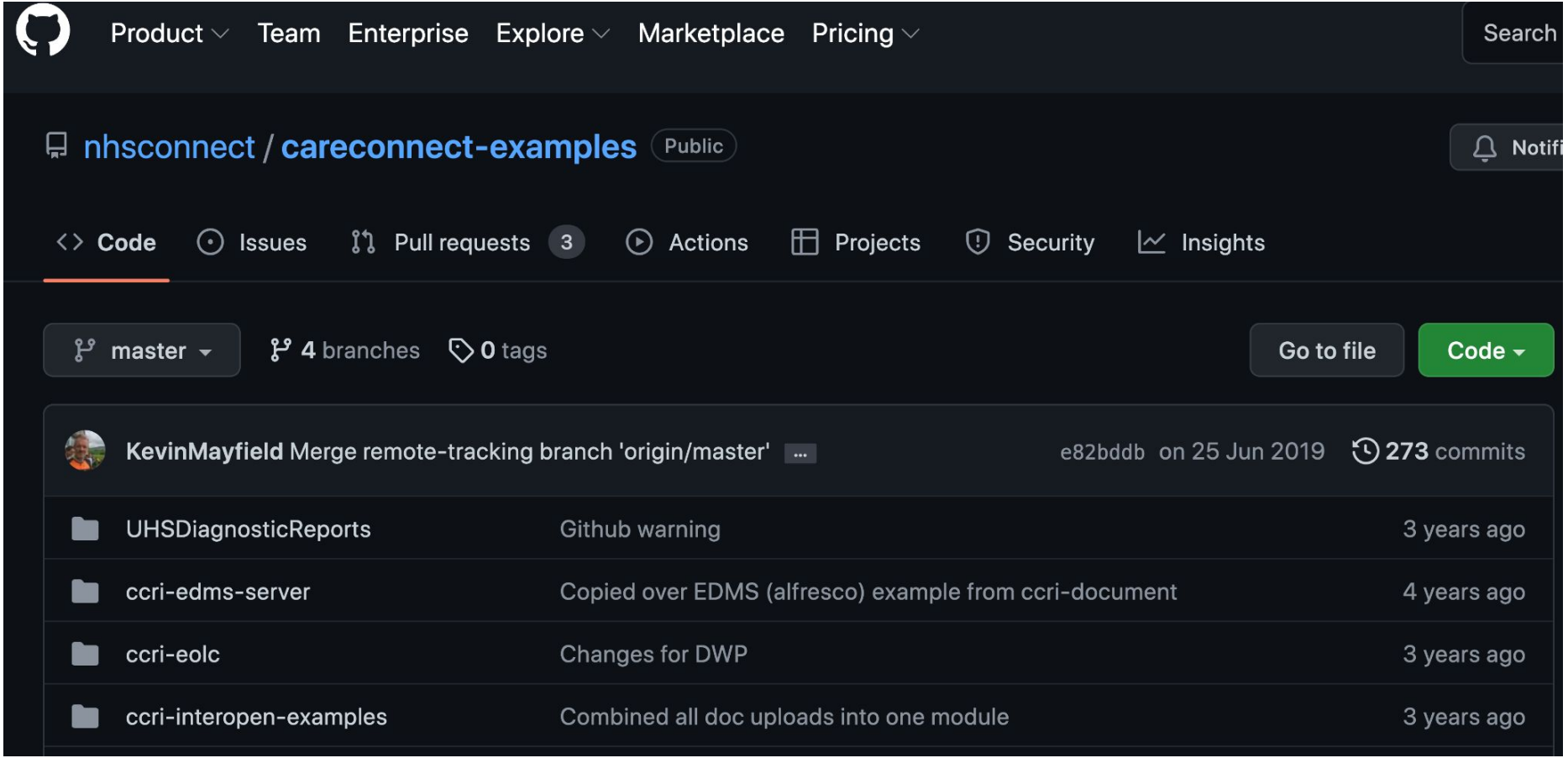


https://developers.google.com/open-health-stack/use-cases

Real World Implementations of FHIR Resources

How UK is Building PHRs on FHIR


Product
Team
Enterprise
Explore
Marketplace
Pricing
Search
NHS Connect
Overview
Repositories 198
Projects
Packages
People 4
Find a repository...
Type
Language
Sort
STU3-FHIR-Assets
Public
Repository for development of NHS Digital STU3 FHIR assets.
Shell 10 8 1 0 Updated 19 minutes ago
prm-repo-pds-adaptor
Public
The PDS-Adaptor is a web service that will communicate with the PDS using the FHIR API to maintain patient details.
Java 0 0 0 0 Updated 13 hours ago

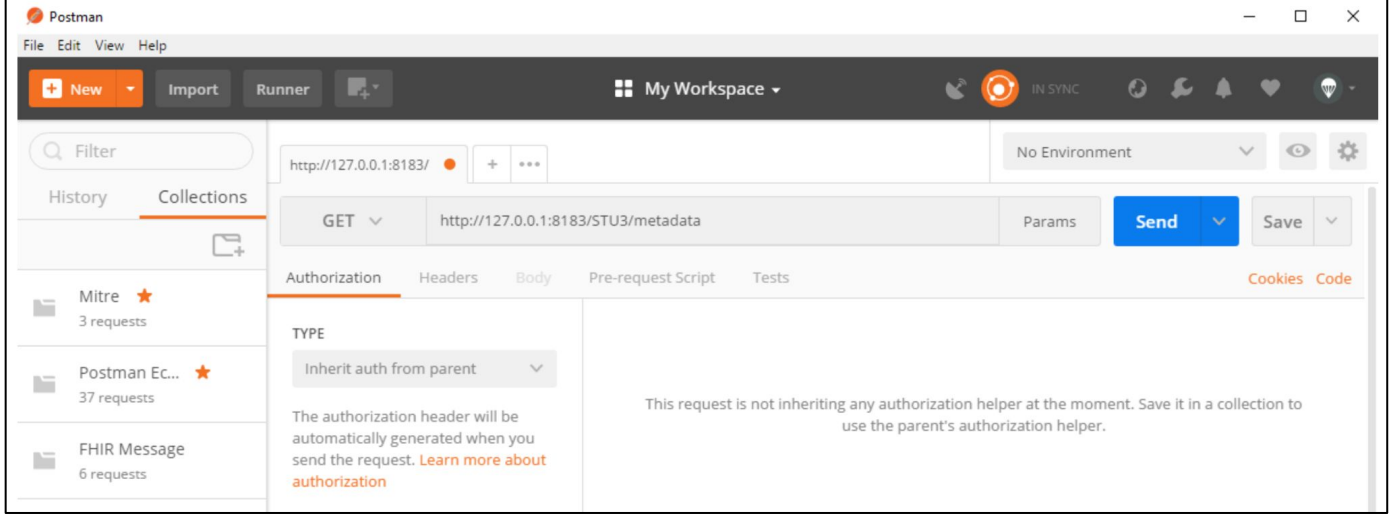

Product
Team
Enterprise
Explore
Marketplace
Pricing
Search
nhsconnect / careconnect-examples
Public
Notifi
Code
Issues
Pull requests 3
Actions
Projects
Security
Insights
master
4 branches
0 tags
Go to file
Code
KevinMayfield Merge remote-tracking branch 'origin/master' ...
e82bddb on 25 Jun 2019
273 commits
UHSDiagnosticReports
Github warning
3 years ago
ccri-edms-server
Copied over EDMS (alfresco) example from ccri-document
4 years ago
ccri-eolc
Changes for DWP
3 years ago
ccri-interopen-examples
Combined all doc uploads into one module
3 years ago

Step 1: Building a FHIR Server

If you followed the pre-requisites and whether you have chosen IntelliJ or Eclipse, you should have a basic FHIR server. To test and confirm, start POSTMan and enter this URL

```
GET http://127.0.0.1:8183/STU3/metadata
```

You should see a FHIR **ConformanceStatement** returned from the server.



https://nhsconnect.github.io/CareConnectAPI/build_patient_server.html

Step 2: Adding a Patient

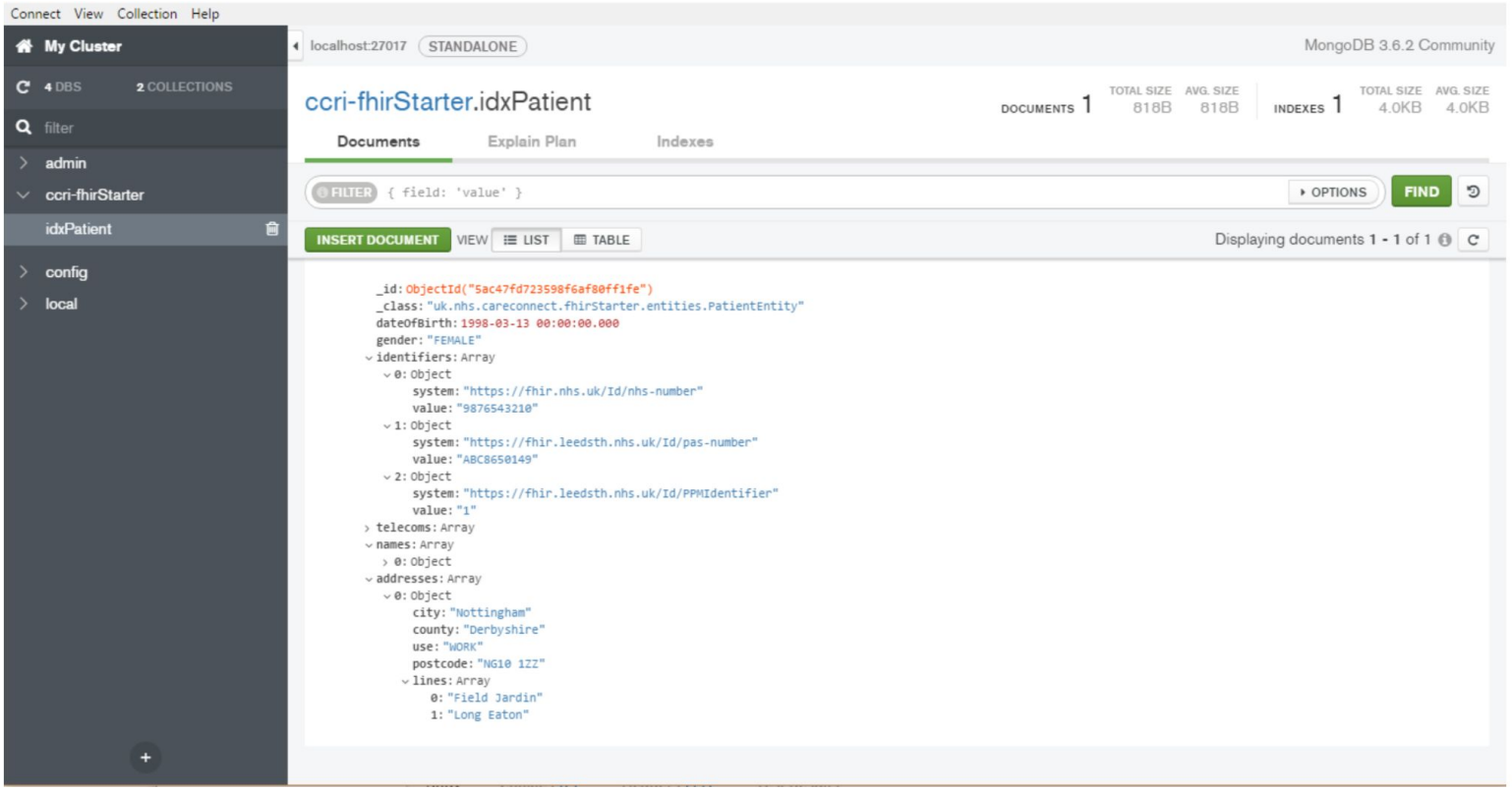
POST http://127.0.0.1:8183/STU3/Patient Params Send Save

Authorization Headers (1) Body Pre-request Script Tests Cookies Code

form-data x-www-form-urlencoded raw binary Text

```
<Patient xmlns="http://hl7.org/fhir">
   <id value="1"/>
   <meta>
      <lastUpdated value="2018-04-03T13:59:40.080+00:00"/>
      <profile value="https://fhir.hl7.org.uk/STU3/StructureDefinition/CareConnect-Patient-1"/>
   </meta>
   <extension url="https://fhir.hl7.org.uk/STU3/StructureDefinition/Extension-CareConnect-EthnicCategory-1">
      <valueCodeableConcept>
         <coding>
            <system value="https://fhir.hl7.org.uk/STU3/CodeSystem/CareConnect-EthnicCategory-1"/>
            <code value="A"/>
            <display value="British, Mixed British"/>
         </coding>
      </valueCodeableConcept>
   </extension>
   <identifier>
      <extension url="https://fhir.hl7.org.uk/STU3/StructureDefinition/Extension-CareConnect-NHSNumberVerificationStatus-1">
         <valueCodeableConcept>
            <coding>
               <system value="https://fhir.hl7.org.uk/STU3/CodeSystem/CareConnect-NHSNumberVerificationStatus-1"/>
               <code value="01"/>
               <display value="Number present and verified"/>
            </coding>
         </valueCodeableConcept>
      </extension>
      <system value="https://fhir.nhs.uk/Id/nhs-number"/>
```

Storing in a Database



Thanks for attending the class!