# HL7® FHIR® Security

## Education Event

Audit Tracing in FHIR

Matt Jenks

8/9/2023

HL7® International

# Who am I?

GigaTECH™

- Chief Technology Officer, GigaTECH
- Software Developer, 30+ years
- Consulting, 10+ years
- Specific interest in Integration, DevSecOps
- Started GigaTECH in 2020 to concentrate on Health IT interoperability
- 2021, CDS & Multi-Domain SMART Apps (payor & provider)

# Intended Audience

- Payors supporting CDS in the clinical workflow
  - Including business product managers, architects, application developers
- Product line managers requiring business metrics
  - Business managers attempting to understand KPIs and application adoption
- Software Developers
  - Architects, Business Analysts, developers, integrators, DevSecOps

# Agenda

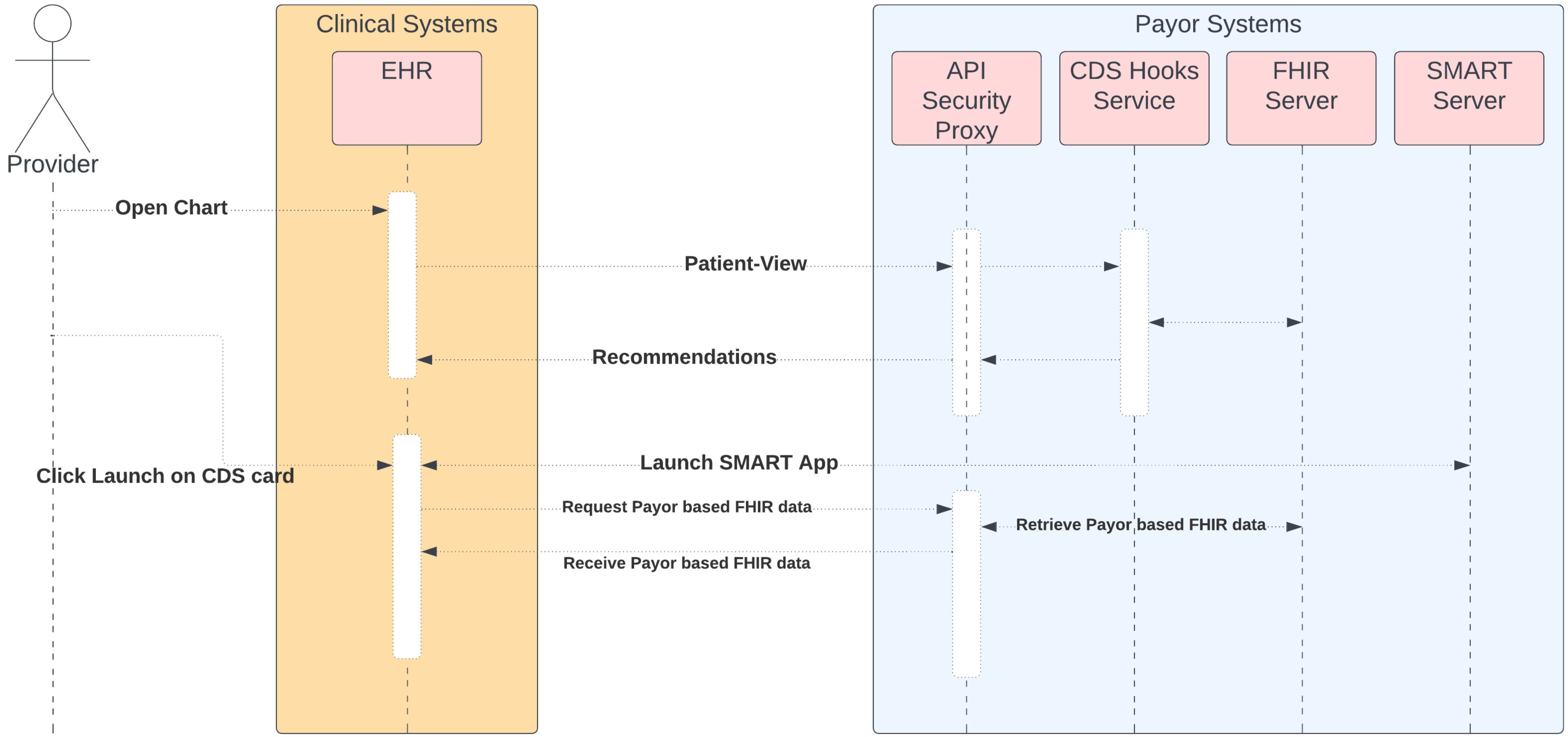
- CDS-Hook and SMART application context
- Metrics and Audit Points
- Constraints
- AuditEvents within the application context
- AuditEvent Visualization

# The CDS Application

- CDS Service
  - Informational Card
  - Makes recommendations based on patient
  - Appears in the EHR as a passive alert

- SMART Application
  - Launched from EHR menu
  - Launched from CDS passive alert
  - Makes it easy for clinician to enroll patient in insurance benefit program

# Application flow



# Metrics and Audit Points

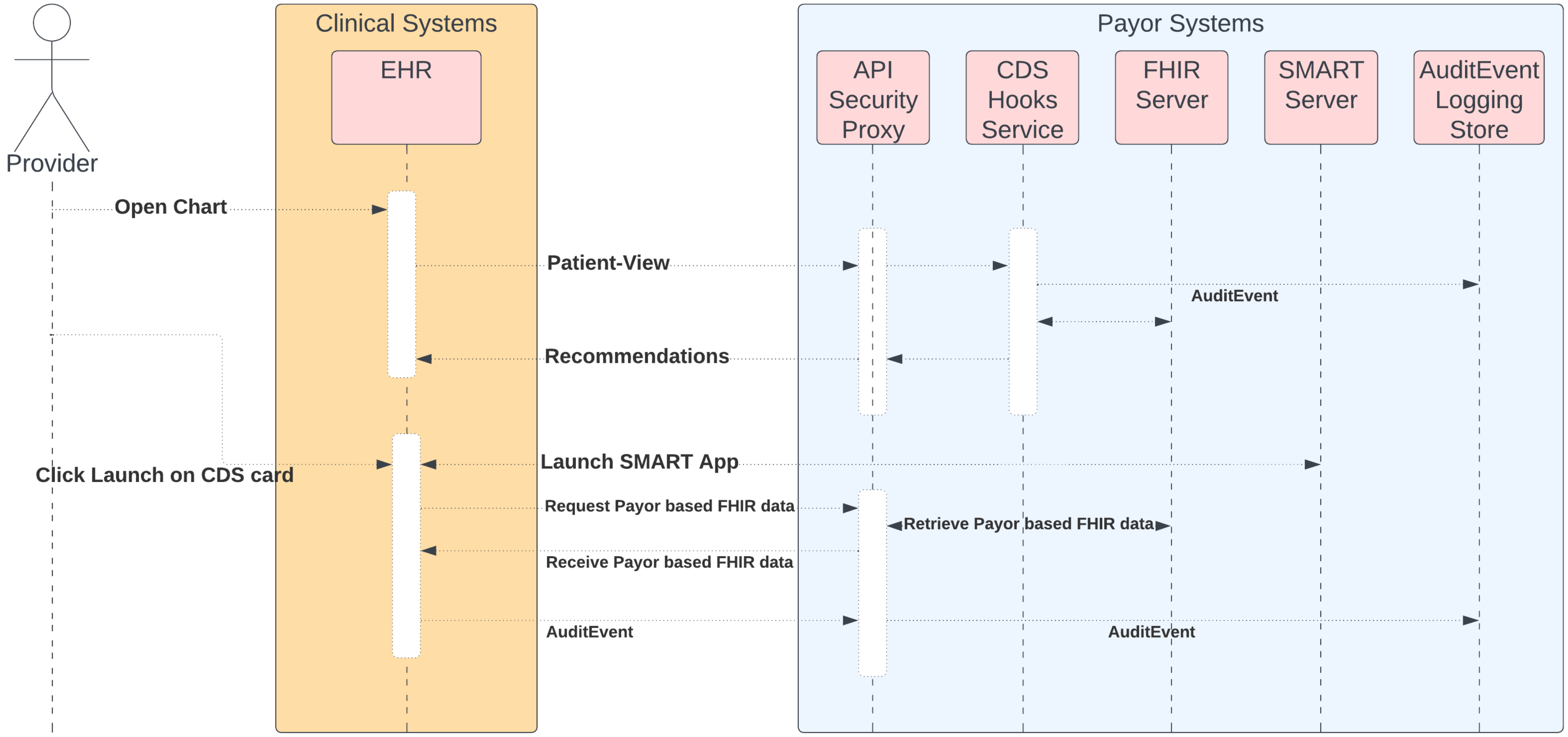
- Business Metrics (KPIs)
  - CDS calls over time
    - Past week, month, quarter
  - SMART Launches over time
    - Total
    - Attributable to CDS
    - By Practitioner
    - By Specialty
  - Enrollments over time
    - Similar to SMART launches over time

- Audit Points
  - Patient/$match response time
    - CDS & SMART
  - CDS Hook response time
    - Possible to affect EHR deployment
  - Payor FHIR server response time
  - Other Payor systems response time

# System Constraints

- FHIR AuditEvents!
- Constraints
  - Data will not include PHI or PII, but can be sensitive
  - Payor did not want to introduce new technologies, if possible
  - Payor required control log over content and where it went
  - Provider and Payor disallowed products like google analytics
  - FHIR Store could not contain AuditEvent data, only clinical or payor data
  - CDS Hook call and SMART application launch were asynchronous

# Application flow with Audit Events



® Health Level Seven and HL7 are registered trademarks of Health Level Seven International, registered with the United States Patent and Trademark Office.

# Basics of Audit Event – describe each section

- Recommend John Meorke’s basic FHIR security class – talks about Audit Event
- Who - .agent(s)
- What - .type, .subtype, .action
- Where - .agent, .entity, .source
- When - .period and .recorded
- Why - .purposeOfEvent
- Created - .entity(s)
- Used - .entity(s)
-

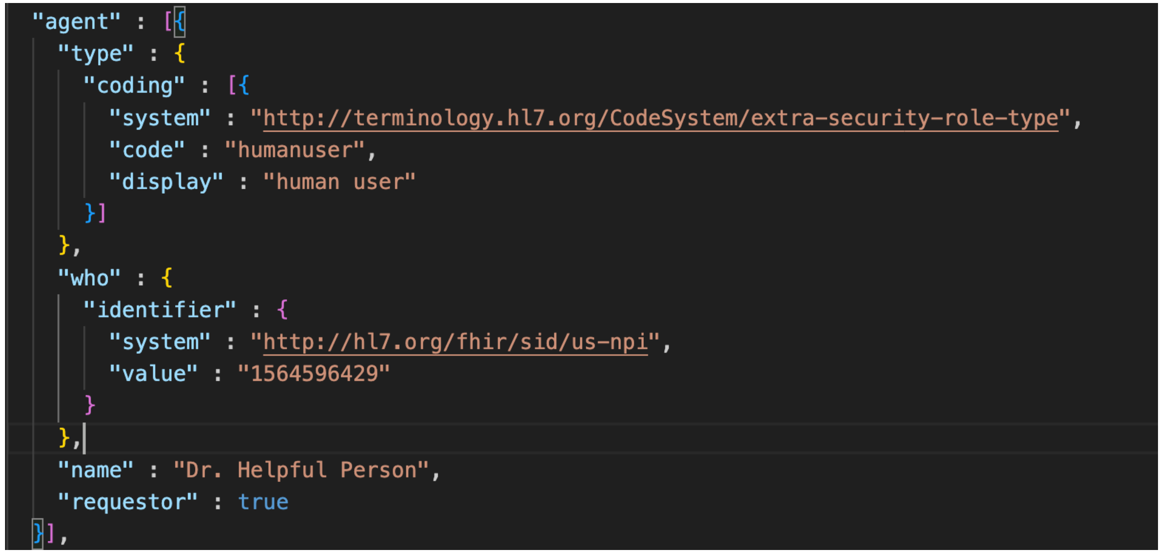
# AuditEvent Basics

- What are we collecting?
  - Who - .agent(s)
  - What - .type, .subtype, .action
  - Where - .agent, .entity, .source
  - When - .period and .recorded
  - Why - .purposeOfEvent
  - Created - .entity(s)
  - Used - .entity(s)

- AuditEvent Spec
  - FHIR R4 AuditEvent
  - http://hl7.org/fhir/R4/auditevent.html
  - GigaTECH examples - https://prom.gigatech.net/docs/artifacts.html
- FHIR Privacy and Security
  - John Moerke
  - http://bit.ly/FHIR-SecPriv

# Audit Event - Who

- What are we collecting?
  - Who - .agent(s)
    - Human
    - NPI
  - What - .type, .subtype, .action
  - Where - .agent, .entity, .source
  - When - .period and .recorded
  - Why - .purposeOfEvent
  - Created - .entity(s)
  - Used - .entity(s)

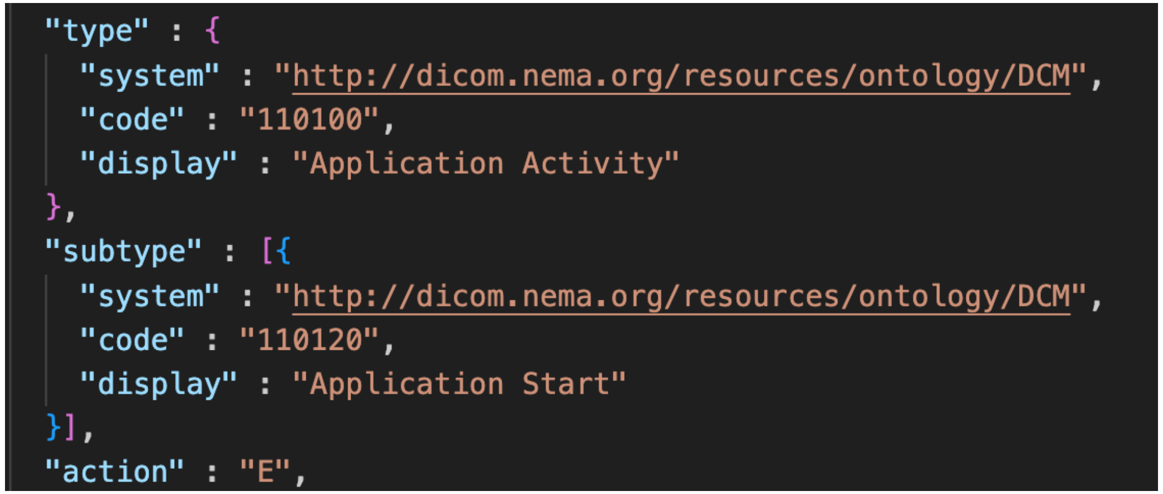


```
"agent" : [{
  "type" : {
    "coding" : [{
      "system" : "http://terminology.hl7.org/CodeSystem/extra-security-role-type",
      "code" : "humanuser",
      "display" : "human user"
    }]
  },
  "who" : {
    "identifier" : {
      "system" : "http://hl7.org/fhir/sid/us-npi",
      "value" : "1564596429"
    }
  },
  "name" : "Dr. Helpful Person",
  "requestor" : true
}],
```

HL7 International

# Audit Event - What

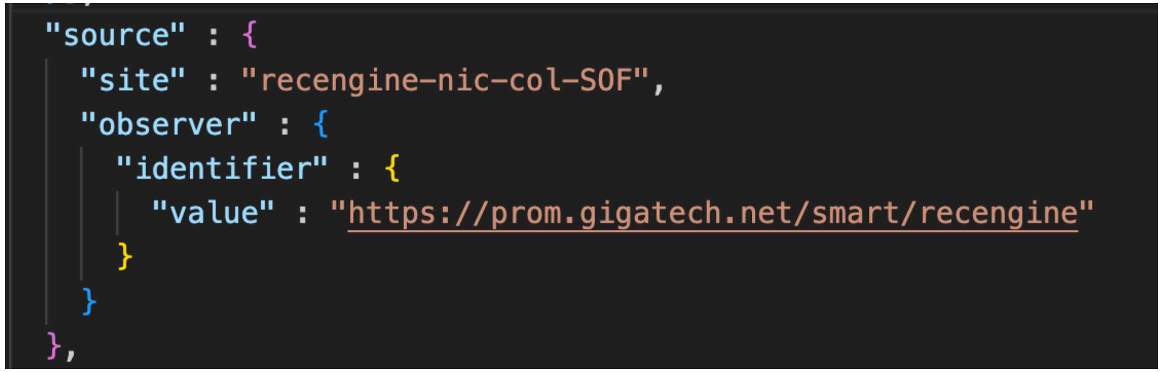
- What are we collecting?
  - Who - .agent(s)
  - What - .type, .subtype, .action
  - Where - .agent, .entity, .source
  - When - .period and .recorded
  - Why - .purposeOfEvent
  - Created - .entity(s)
  - Used - .entity(s)



```
"type" : {
  "system" : "http://dicom.nema.org/resources/ontology/DCM",
  "code" : "110100",
  "display" : "Application Activity"
},
"subtype" : [{
  "system" : "http://dicom.nema.org/resources/ontology/DCM",
  "code" : "110120",
  "display" : "Application Start"
}],
"action" : "E",
```

# Audit Event - Where

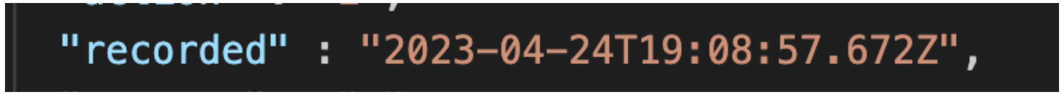
- What are we collecting?
  - Who - .agent(s)
  - What - .type, .subtype, .action
  - Where - .agent, .entity, .source
  - When - .period and .recorded
  - Why - .purposeOfEvent
  - Created - .entity(s)
  - Used - .entity(s)



```
"source" : {
  "site" : "recengine-nic-col-SOF",
  "observer" : {
    "identifier" : {
      "value" : "https://prom.gigatech.net/smart/recengine"
    }
  }
},
```

# Audit Event - When

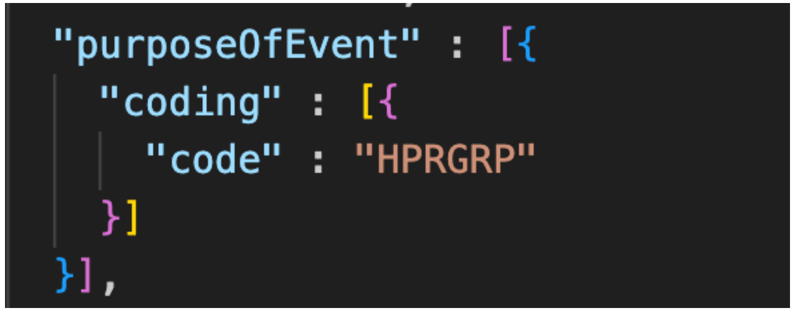
- What are we collecting?
  - Who - .agent(s)
  - What - .type, .subtype, .action
  - Where - .agent, .entity, .source
  - When - .period and .recorded
  - Why - .purposeOfEvent
  - Created - .entity(s)
  - Used - .entity(s)



```
"recorded" : "2023-04-24T19:08:57.672Z",
```

# Audit Event - Why

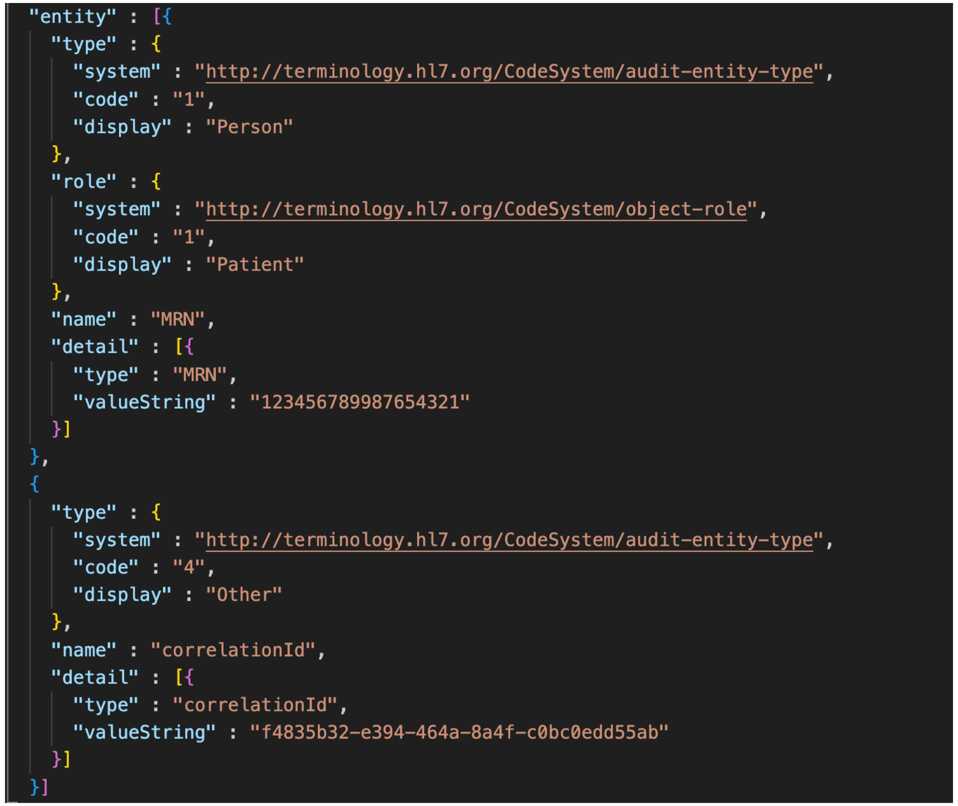
- What are we collecting?
  - Who - .agent(s)
  - What - .type, .subtype, .action
  - Where - .agent, .entity, .source
  - When - .period and .recorded
  - Why - .purposeOfEvent
  - Created - .entity(s)
  - Used - .entity(s)



```
"purposeOfEvent" : [{
  "coding" : [{
    "code" : "HPRGRP"
  }]
}],
```

# Audit Event – Created/Used

- What are we collecting?
  - Who - .agent(s)
  - What - .type, .subtype, .action
  - Where - .agent, .entity, .source
  - When - .period and .recorded
  - Why - .purposeOfEvent
  - Created - .entity(s)
  - Used - .entity(s)
    - Patient
    - Correlation Id



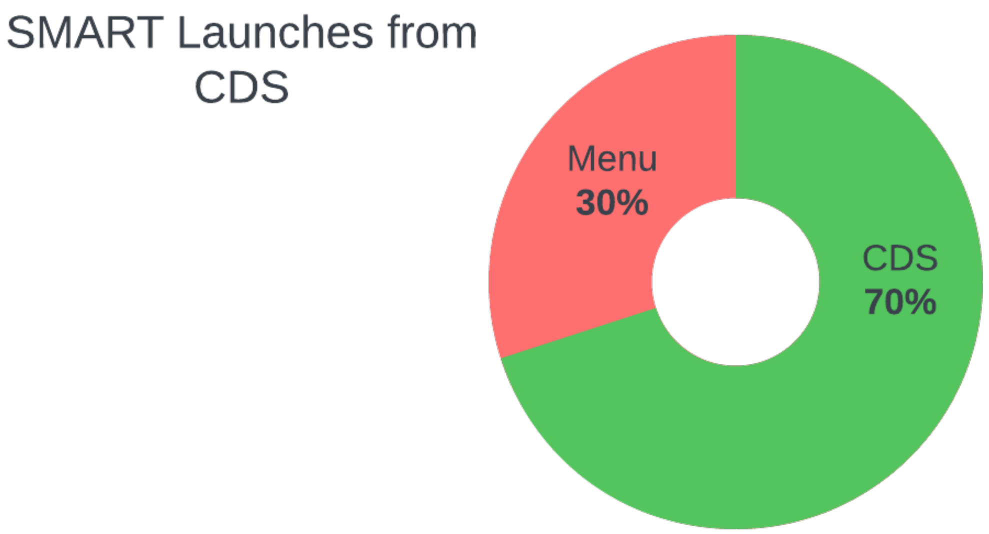
```
"entity" : [{
  "type" : {
    "system" : "http://terminology.hl7.org/CodeSystem/audit-entity-type",
    "code" : "1",
    "display" : "Person"
  },
  "role" : {
    "system" : "http://terminology.hl7.org/CodeSystem/object-role",
    "code" : "1",
    "display" : "Patient"
  },
  "name" : "MRN",
  "detail" : [{
    "type" : "MRN",
    "valueString" : "123456789987654321"
  }]
},
{
  "type" : {
    "system" : "http://terminology.hl7.org/CodeSystem/audit-entity-type",
    "code" : "4",
    "display" : "Other"
  },
  "name" : "correlationId",
  "detail" : [{
    "type" : "correlationId",
    "valueString" : "f4835b32-e394-464a-8a4f-c0bc0edd55ab"
  }]
}]
```

# Audit Event Visualization

- KPIs (slide 7)
  - CDS calls over time
    - Past week, month, quarter
  - SMART Launches over time
    - Total, past week, month, quarter
    - Attributable to CDS
    - By Practitioner
    - By Specialty
  - Enrollments over time
    - Similar to SMART launches over time

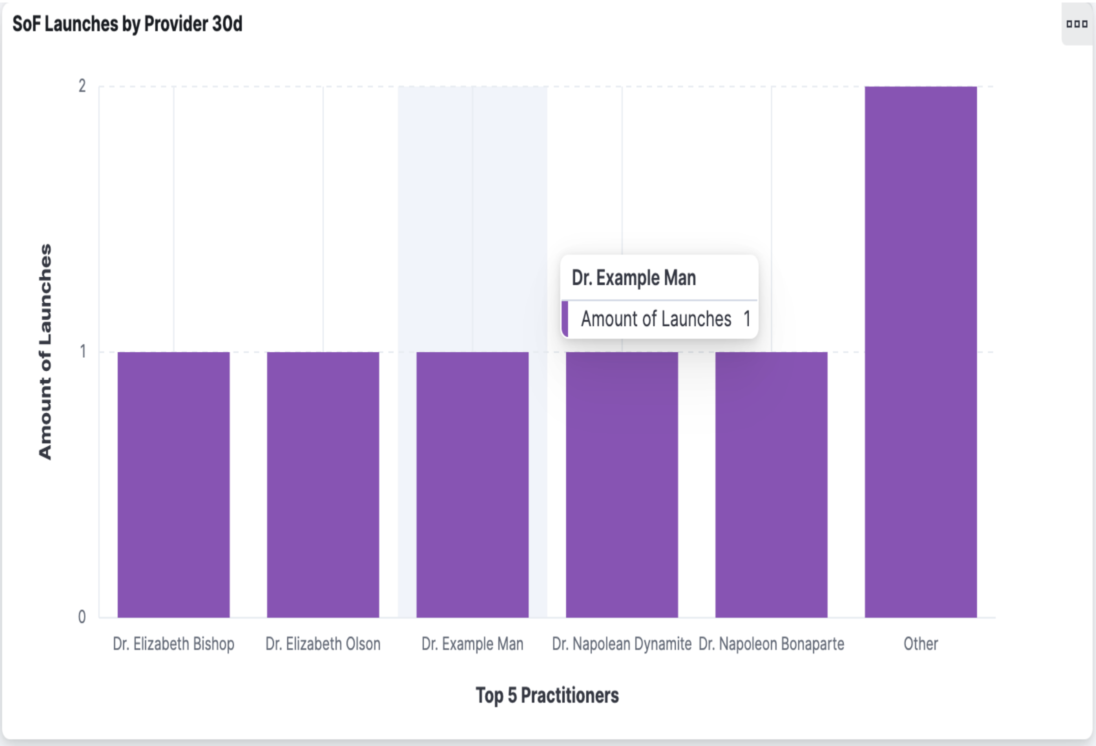
# Audit Event Visualization – CDS & SMART

- KPIs (slide 7)
  - CDS calls over time
    - Past week, month, quarter
  - SMART Launches over time
    - Total, past week, month, quarter
    - Attributable to CDS
    - By Practitioner
    - By Specialty
  - Enrollments over time
    - Similar to SMART launches over time



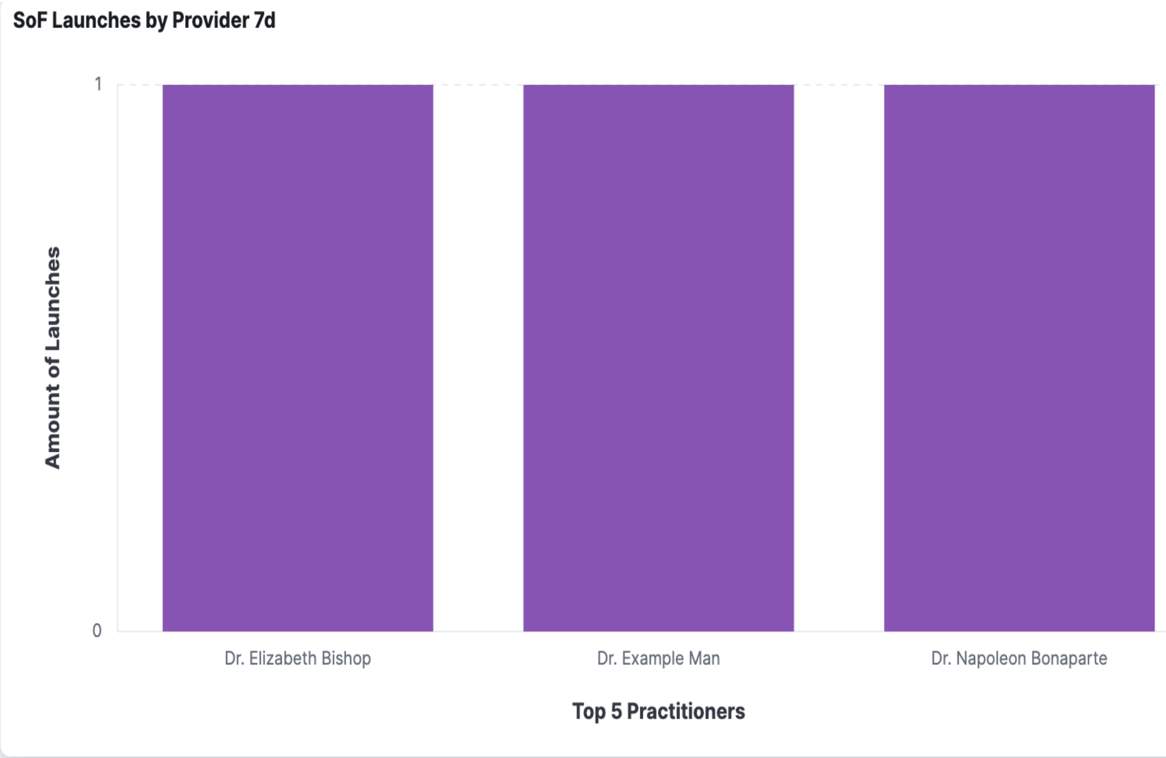
# Audit Event Visualization – Practitioners

- KPIs (slide 7)
  - CDS calls over time
    - Past week, month, quarter
  - SMART Launches over time
    - Total, past week, month, quarter
    - Attributable to CDS
    - By Practitioner
    - By Specialty
  - Enrollments over time
    - Similar to SMART launches over time



# Audit Event Visualization – Practitioners

- KPIs (slide 7)
  - CDS calls over time
    - Past week, month, quarter
  - SMART Launches over time
    - Total, past week, month, quarter
    - Attributable to CDS
    - By Practitioner
    - By Specialty
  - Enrollments over time
    - Similar to SMART launches over time



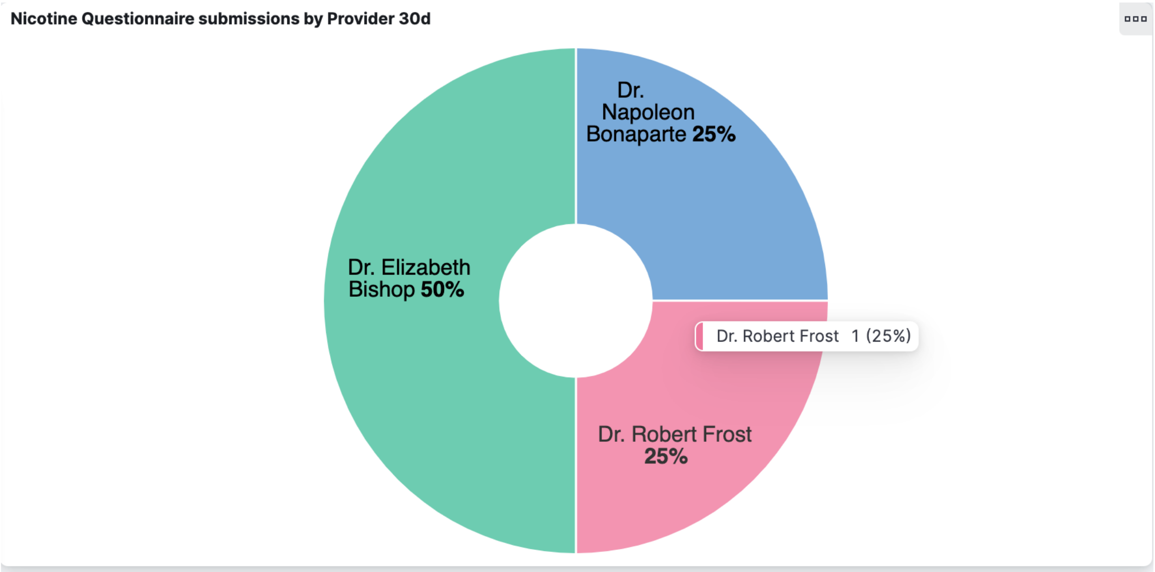
# Conclusion

Questions?

# Backup Slides

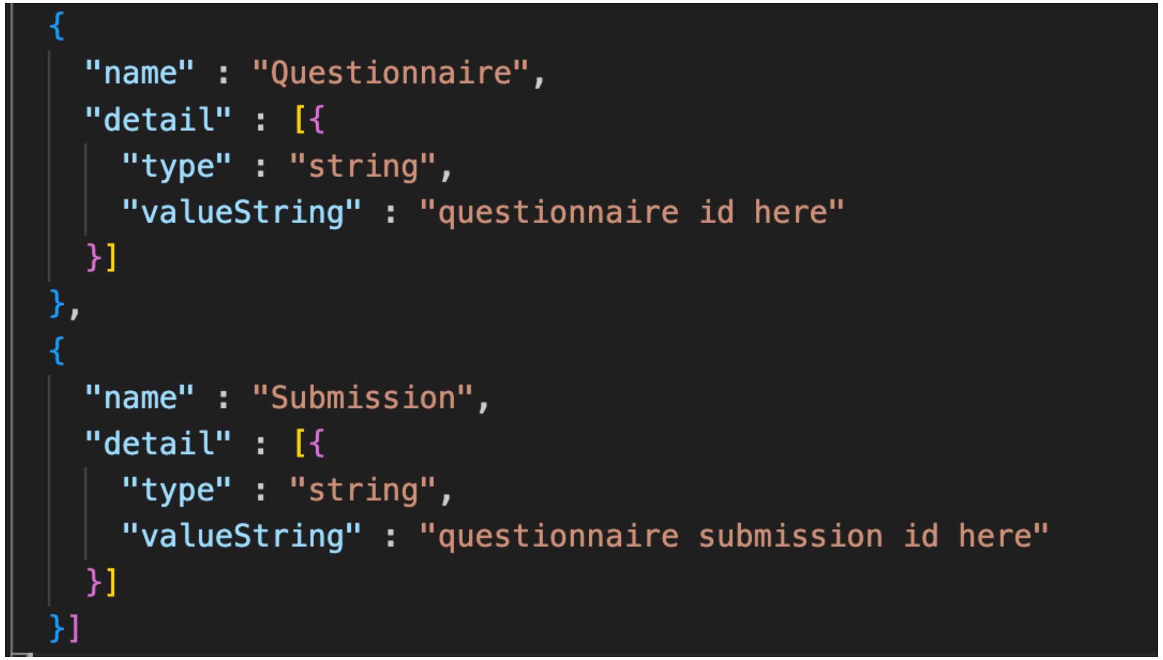
# Audit Event Visualization – Enrollments

- KPIs (slide 7)
  - CDS calls over time
    - Past week, month, quarter
  - SMART Launches over time
    - Total, past week, month, quarter
    - Attributable to CDS
    - By Practitioner
    - By Specialty
  - Enrollments over time
    - Similar to SMART launches over time


Nicotine Questionnaire submissions by Provider 30d

# Audit Event Visualization – Enrollments

- Enrollments
  - For instance, questionnaire submission
  - Part of entity array



```
{
  "name" : "Questionnaire",
  "detail" : [{
    "type" : "string",
    "valueString" : "questionnaire id here"
  }]
},
{
  "name" : "Submission",
  "detail" : [{
    "type" : "string",
    "valueString" : "questionnaire submission id here"
  }]
}]
```