# Fine-grained security policies

FHIR DevDays June 2020

https://bit.ly/fhir20-fine

# Panelists

- Michael Hansen PhD, Principal PM at Microsoft Healthcare
- Christiaan Knaap, Lead Developer for Vonk, Firely
- Josh Mandel MD, Chief Architect at Microsoft Healthcare
- Nikolai Ryzhikov PhD, CTO at Health Samurai

https://bit.ly/fhir20-fine

# Use cases

- Consumer application access
- HIPAA minimum necessary for provider-facing apps
- Controlled access for client-side apps
- Sharing data with researchers according to consent

https://bit.ly/fhir20-fine

# Themes for discussion

- Architecture: where do policy definition & enforcement live?
- Identity: where do users & their permissions live?
- Resource-level control: thinking beyond FHIR Compartments
- Sub-resource control: thinking beyond FHIR _elements
- Expanding the conversation: symposium, interest group, etc?

https://bit.ly/fhir20-fine

# Background: authz API standards efforts ... beyond (vanilla) OAuth

- OAuth Rich Authorization Requests
- User Managed Access (UMA 2.0)
- OAuth.xyz

https://bit.ly/fhir20-fine

# OAuth Rich Authorization Requests

See draft spec.

Adds "**authorization_details**" as a kind of improved "scope" parameter

Extensible schema for these details, with "**type**", "**datatypes**", and "**actions**"...

```
[{
 "type": "fhir",
  "locations": [
    "https://fhir.example.com/clinical",
    "https://fhir.example.com/imaging"
  ],
  "actions": [
    "Read",
    "Search"
  ],
  "datatypes": [
    "Patient",
    "Observation"
  ],
  ...
```

https://bit.ly/fhir20-fine

# User Managed Access (UMA 2.0)

See published spec.

- Separate the role of resource server from authorization server
- Put the authorization server under the user's control
- Separate the role of user from "requesting party"
- Resource server tells authorization server what resources exist
  - Resource name
  - List of scopes
- Apps requesting access get a "permission ticket"
  - List of resources
  - For each resource, a list of scops

https://bit.ly/fhir20-fine

# OAuth.xyz

See proposed spec.

- Ground-up new protocol (not OAuth 2.0 compatible)

- Flexible separation of
  - Requests (who is asking for what?)
    - Includes a schema similar to OAuth RAR proposal
  - Interactions
    - Can a decision be rendered automatically?
    - Is there a user here who can provide details or permissions?
  - Responses (what is being granted? How can a resource server check?)
  - Tokens (including bearer tokens and client-bound tokens, via public keys)

https://bit.ly/fhir20-fine

# Scenarios

- Patients can access their own data
  - What is “their own data”? Do nursing notes belong to a patient?
  - In case of write access any validation on proper link to this patient in resource?
- Practitioner can see patients in his department
  - Nurses should not see SSN
  - Physician could not see mental problems
- Practitioner can access records of “her patients”
- Parents can see their child's medical record
  - E.g., Until age 16
  - E.g., Excluding subsets
- Patient want to share narrowed scope of his data to somebody
- Nurse can update part of Encounter resource

choose your AS

choose your db