UMA Workgroup

- Why UMA?
- How?
- UMA Capabilities
- Recent & Future Work
- Contacts & References

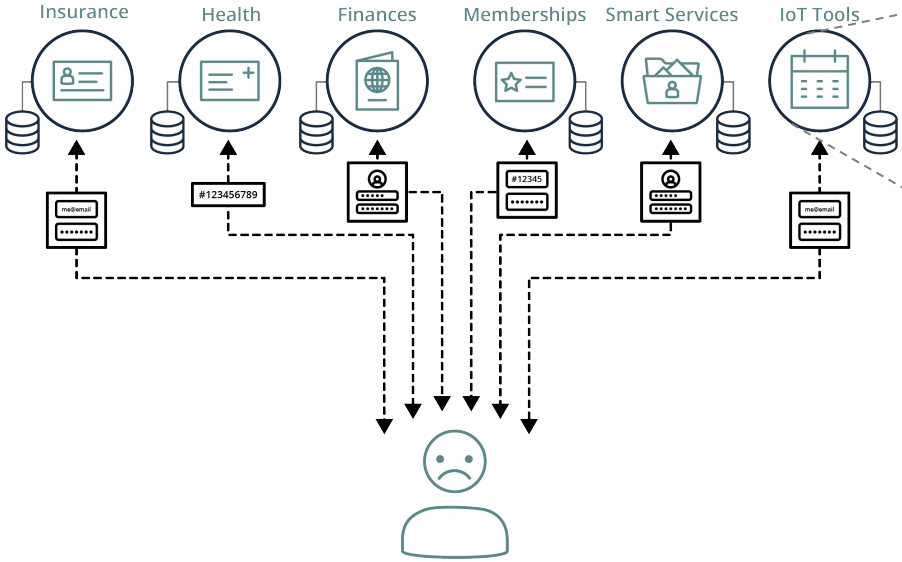
Master Deck located in ForgeRock GDrive here
Feel free to reach out to Steve.Venema@ForgeRock.com for access

Why UMA?

The Usual Walled Gardens

Difficult to share your data with others

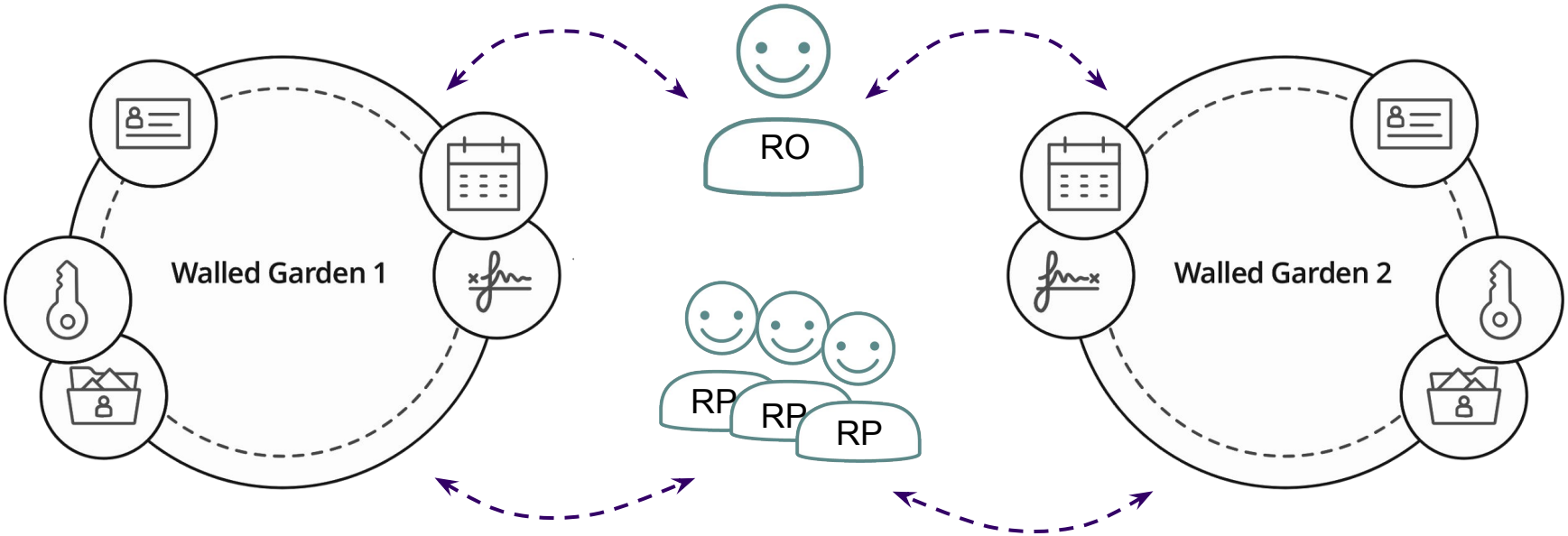
120 Walled Gardens – 1 identity at a time



Me online **x 120**!

How can I selectively share access to my data and services with others?

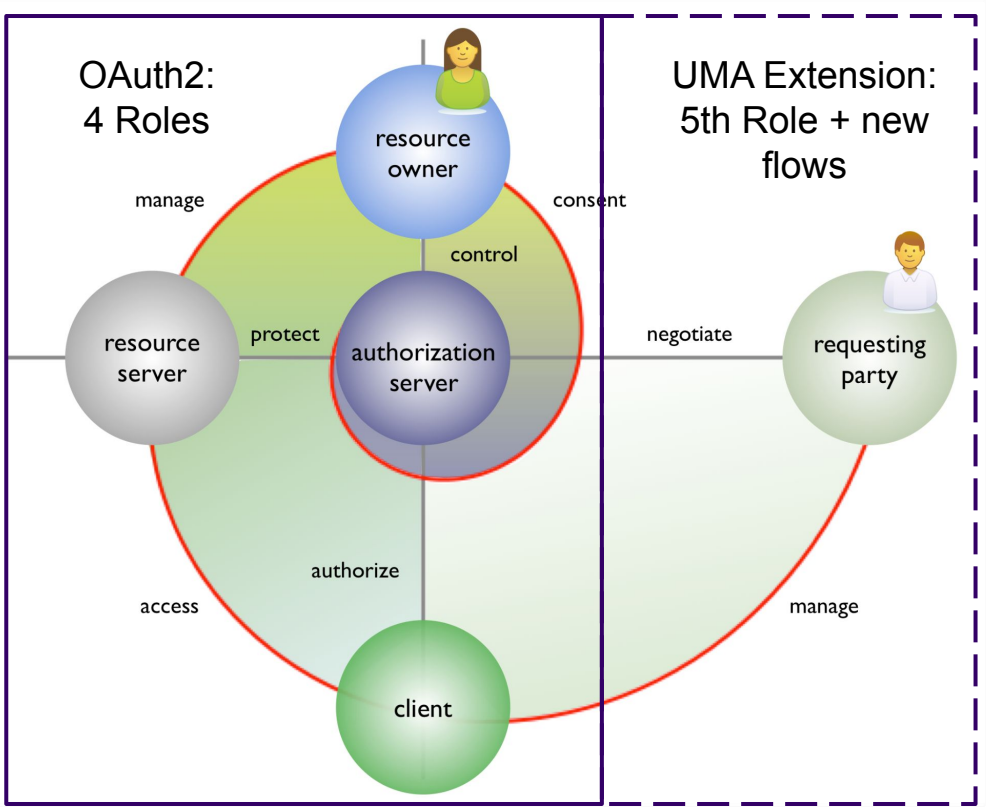
We Can Do Better



What if... we can create a user centered ecosystem that makes it simple to share your data with others?

How does UMA accomplish this?

UMA 2.0: Extension to OAuth2



- Adds **party-to-party authorization** rather than authorization of application access alone
- Supports **Asynchronous authorization**: RO doesn't need to be online for RP to request access
- Optional FedAuthZ spec allows **loose coupling between AS and RS** from RO perspective
- Aligned with OIDC; VC friendly as well

UMA Enables User-Centric Delegation

Delegation of Access

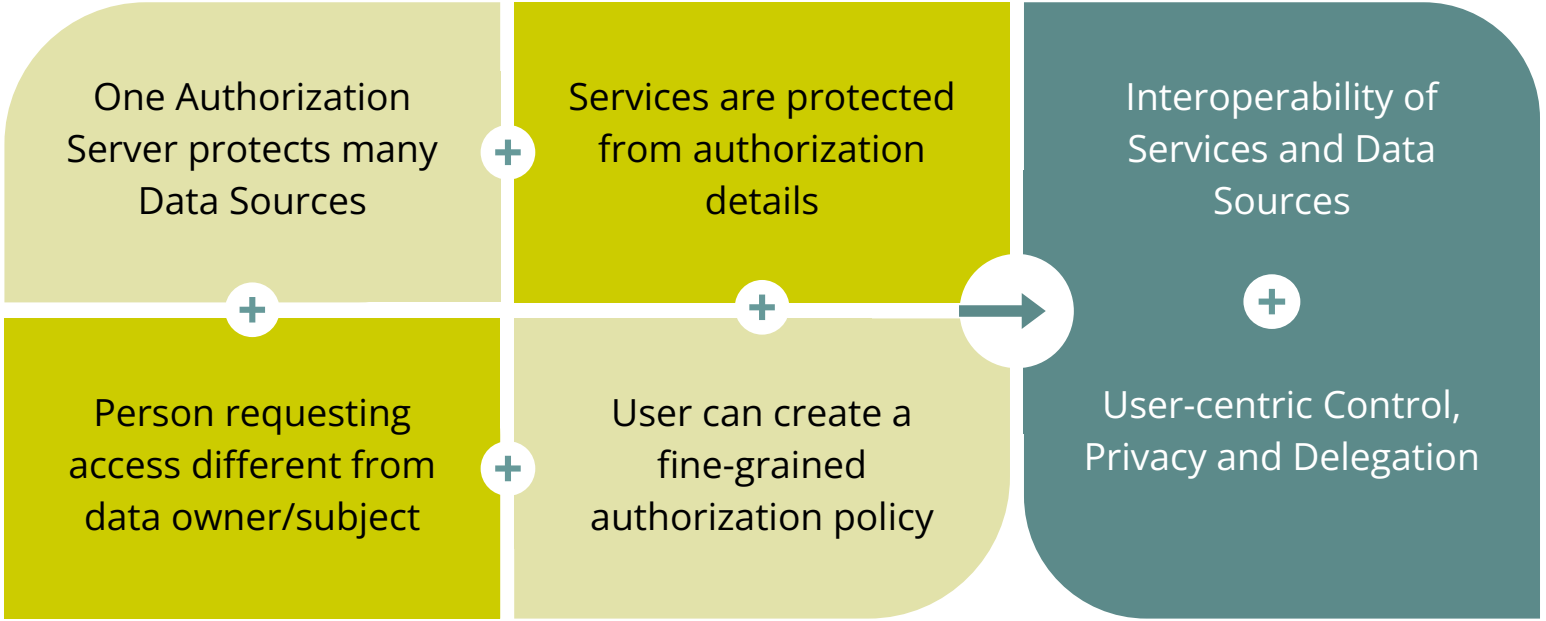
- RO defines rules for RPs' access RO's resources
- RPs may asynchronously request/gain access to RO resources
  - Online presence of RO not required
- Ex: medical records, financial transactions, government services

Architecture

- One AS can protect many RS, one RS can trust many AS
- AS and RS are decoupled
- Services decoupled from authZ details via a standard interface
- Agnostic to resource data types

Resulting Capabilities

UMA Capability Summary



Effects of Deploying UMA

- Creates **wide-ecosystems** by loosely coupling resources to authorization
- Remains **Identity agnostic** by working with existing IAM systems and user accounts
- **Leverages existing standards** such as OAuth2 & OIDC
- **User-centric experience** for sharing personal data and services with others

Implementations

ForgeRock – financial, healthcare, IoT, G2C…
Gluu (OSS) – API protection, enterprise,…
HIE of One / Trustee (OSS) – healthcare
IDENTOS – healthcare, G2C,
PatientShare – healthcare
HealthyMePHR – healthcare
Pauldron (OSS) – healthcare
RedHat Keycloak (OSS) – API protection, enterprise, IoT…
WSO2 (OSS) – enterprise

Example Deployments

UK Pensions Dashboard

Ontario Trusted Account

Trustsphere @ BC Children's Hospital

UMA WG Recent & Future Work

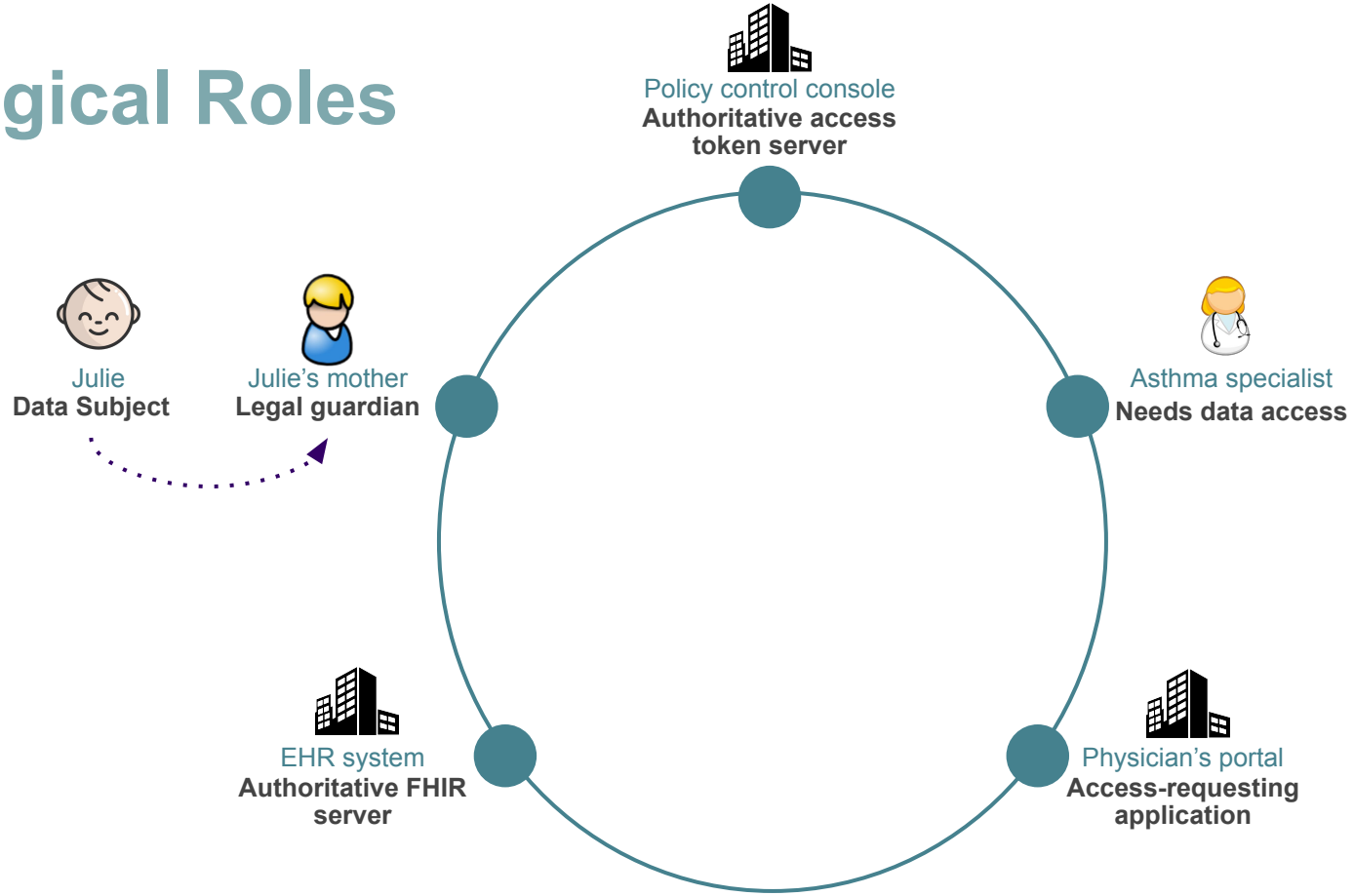
Patient-Centric Data Sharing with UMA

The Julie Adams Healthcare Use Case from the Protecting Privacy to Promote Interoperability Work Group

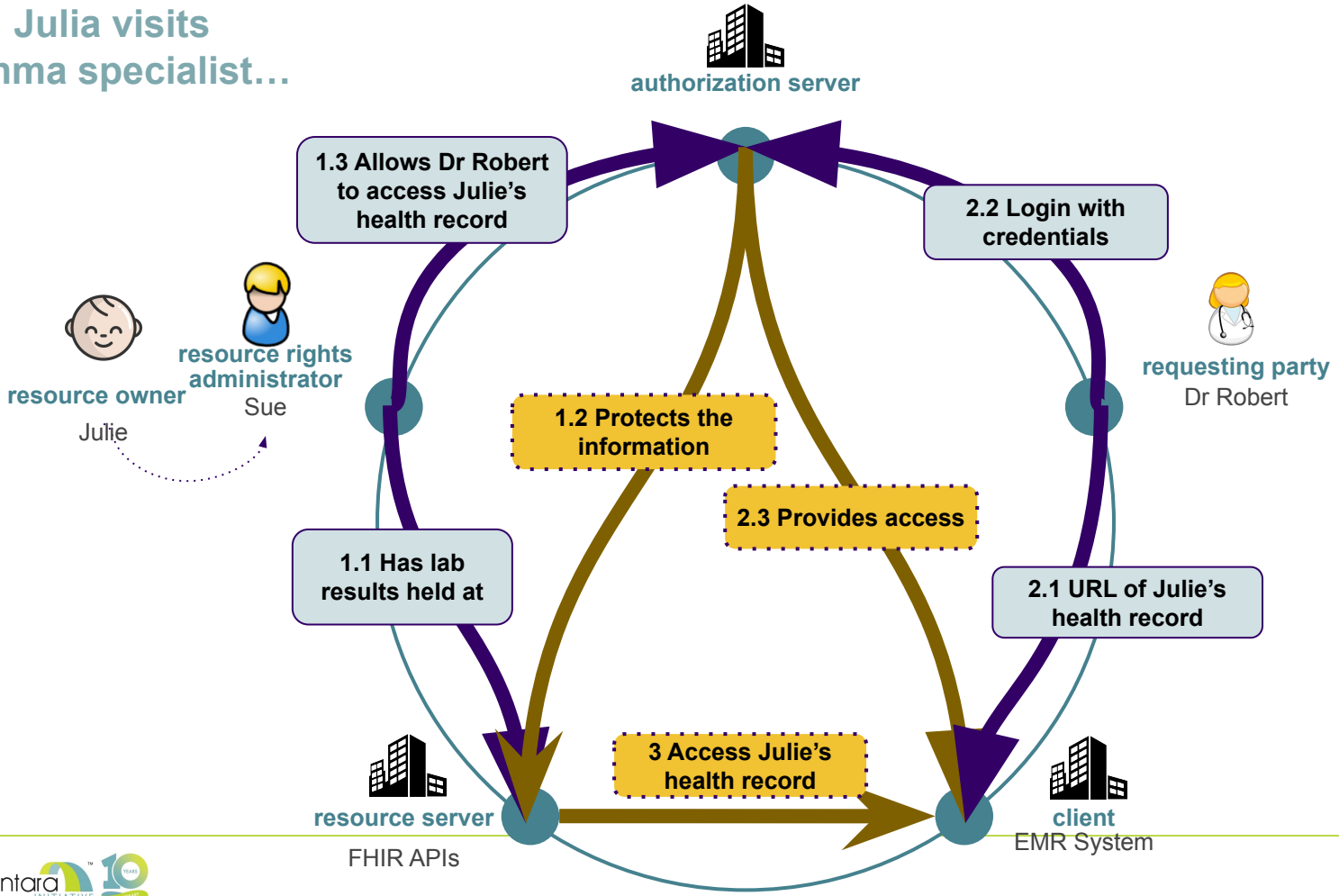
Abstract: This Draft Report analyzes the "Adolescent" (Julie Adams) use case for granularly segmenting personal health data, developed by Protecting Privacy to Promote Interoperability (PP2PI), and assessing ways the User-Managed Access (UMA) protocol can address this challenge.

Link: Current Draft

Logical Roles



Julia visits asthma specialist…



Future Work: 2022+ Plan

Open Banking use-case (Report)

UMA, UDAP, etc. comparison & alignment work

UMA adoption

Contacts & References

More Information About UMA

Join us! We meet every Thursday

UMA WG Home:

https://kantarainitiative.org/confluence/display/uma/Home

Learn the “How” of UMA:

UMA 2:0 Deep Dive: Applying User-Managed Access | Identiverse 2018:
https://www.youtube.com/watch?v=0cCXJvJ6GUY

UMA Specs and Auxiliary Documents:
https://kantarainitiative.org/confluence/display/uma/Specifications+and+Auxiliary+Documents

Backup Slides

Use case: Ontario trusted account

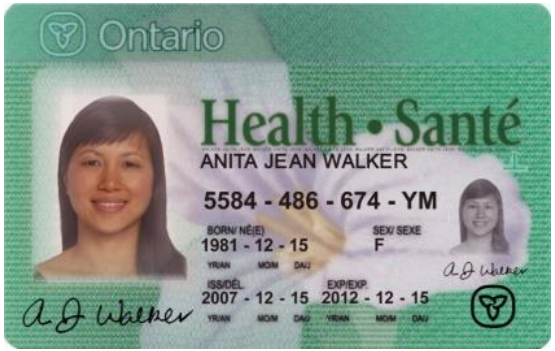
What impact will patient digital access have?

Digitally access personal health information (e.g. lab test results, prescription information), book appointments and track referrals.

Interact virtually with a health care provider via video visit or secure messaging.

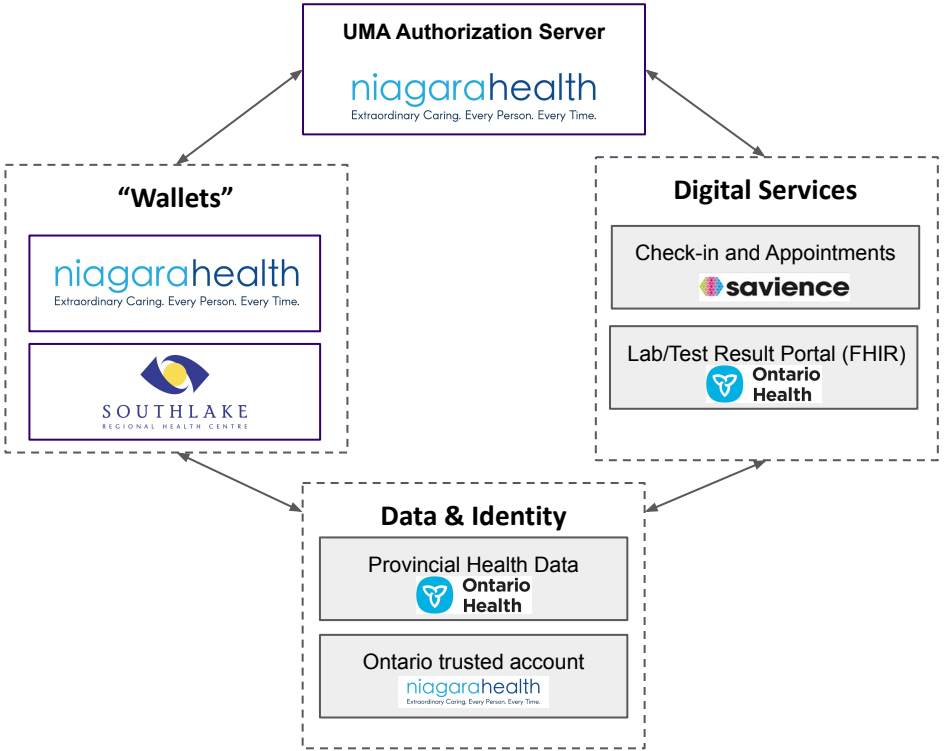
Digitally share important information with their health care provider(s).

Digitally ensure that patients control access to their data through consent and access controls.

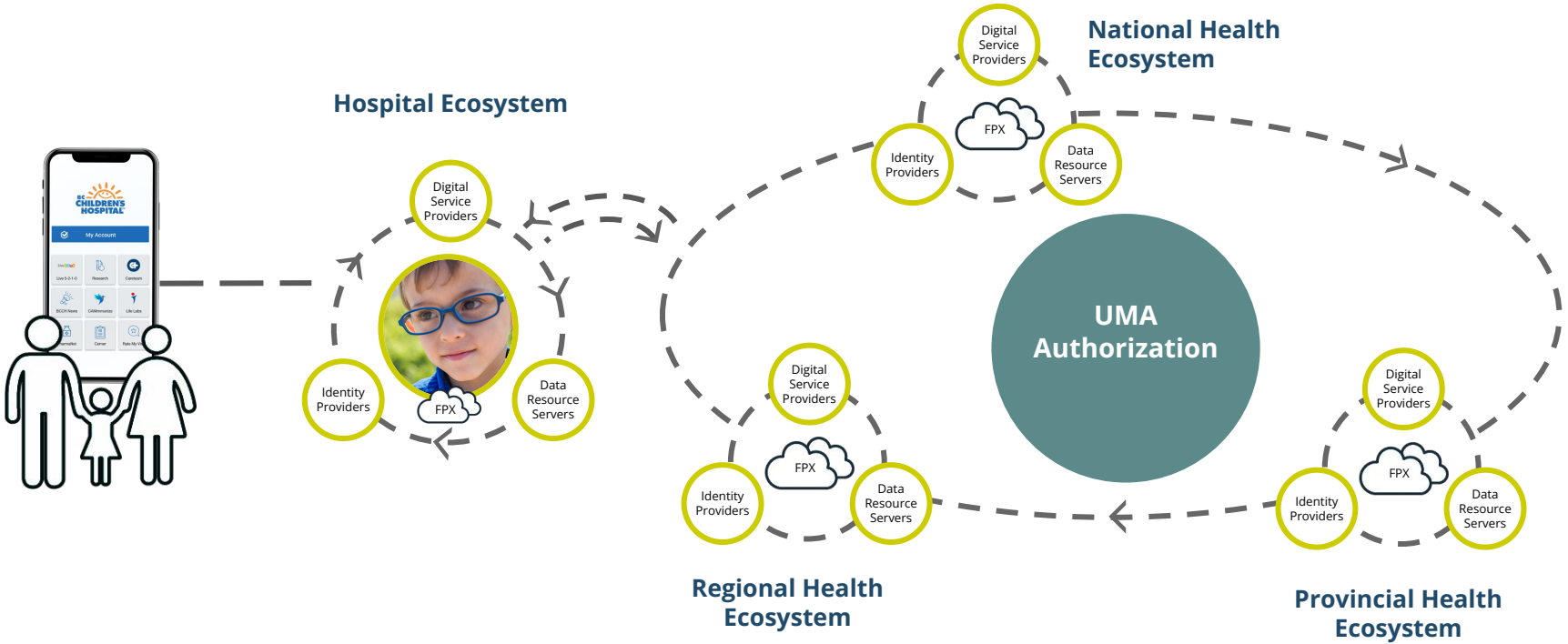


Ontario trusted account

- Ontario Health Card Holders can
  - create a verified identity resource and protect it at an UMA AS
  - discover and protect their health information from a single place
  - digitally access personal health information
  -



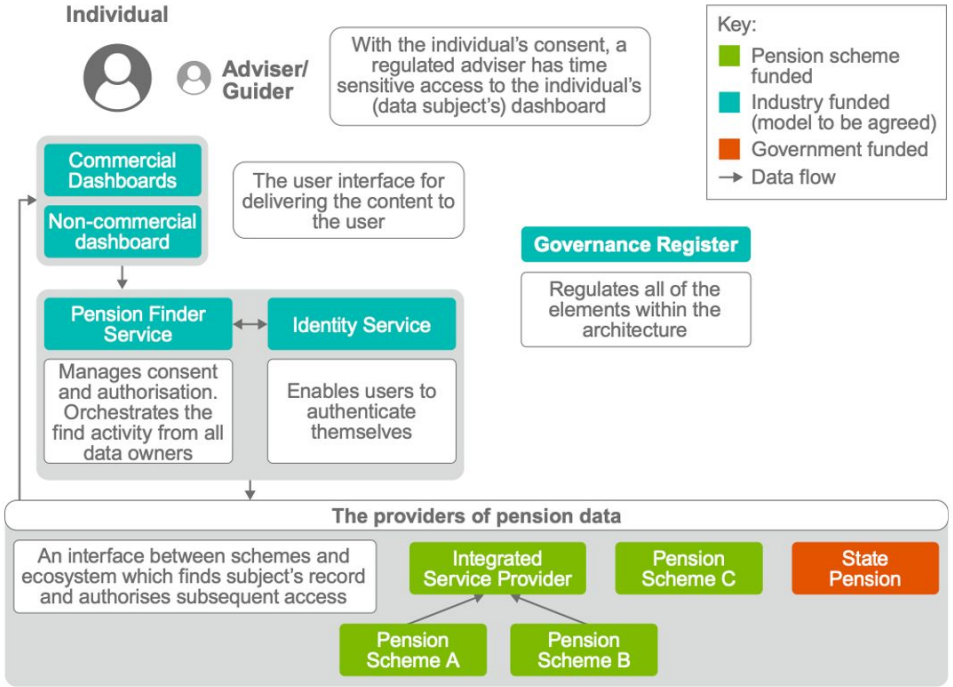
Connecting Healthcare Journeys in Canada



Use case: UK Pensions Dashboard

UK Pensions Dashboard

- UK Pension Holders can
  - discover and protect pension resources
  - see a single dashboard of all pensions
  - delegate access to advisors
- UMA profile created by Origo



PDP Progress update report: October 2020

DWP Proposed ecosystem