

# Patient-Centric Data Sharing with UMA

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

**Version:** 0.3

**Editor:** Nancy Lush, Alec Laws, Eve Maler

**Contributors:** Anik Chawla, Sal D'Agostino, Scott Fehrman, Steven Venema

**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.

**Status of This Document:** This is an Working Group Draft Report produced by the [User-Managed Access \(UMA\) Work Group](#). See the [Kantara Initiative Operating Procedures](#) for more information. Additional contributors to this report include the Kantara UMA Work Group participants, a list of whom can be found [here](#).

**Copyright Notice:** Copyright © 2022 Kantara Initiative and the persons identified as the document authors. All rights reserved. This document is subject to the [Kantara IPR Policy - Option Patent & Copyright: Reciprocal Royalty Free with Opt-Out to Reasonable And Non discriminatory \(RAND\) \(HTML version\)](#).

1. Why Read This Report	3
2. The Adolescent Use Case and Its Data Sharing Implications	3
3. The Nuts and BOLTS of Policy and How It Impacts Julie’s Journey	5
4. Overview of UMA and HEART and Their Relationship to FHIR	5
5. OAuth and UMA	7
6. Basic UMA Use Case	8
7. Delegating Control of Access Rights	11
8. Applying UMA to Julie’s Story	13
9. Julie Begins Self-Administration of Her Clinical Data	14
10. Julie’s Record Collects More Sensitive Data as She Matures	15
11. Granular Sharing of Julie’s Data Using UMA and HEART	15
12. Conclusion	17
A. PP2PI Scenario Assumptions and Simplifications	18
B. About This Report and the Standards Mentioned	18
C. Other Related Technologies	19

## 1. Why Read This Report

The Protecting Privacy to Promote Interoperability (PP2PI) Workgroup, an interest group of expert stakeholders across the healthcare industry, is working to promote patient care equity and safety by providing implementation guidance for the granular segmentation of sensitive data. PP2PI has developed several use cases to illustrate the many challenges involved in this complex problem, as well as solutions.

The User-Managed Access (UMA) standard supports PP2PI's core goal of securely sharing clinical data while protecting patient privacy. This report delves into the PP2PI "Adolescent" use case, personified by "Julie Adams." We explain which specific problems can be best solved with UMA and the benefits of taking this approach.

Acknowledging that the problem space includes many business, operational, legal, technical, and societal aspects, we identify which aspects are in scope or out of scope for UMA. As an example, we won't take a stance on what policy would be appropriate, but rather given a certain policy, how that policy will be enforced.

**Summary:** The "Adolescent" use case proposed by PP2PI is complex. This report analyzes key aspects of the use case that are amenable to technology solutions and proposes User-Managed Access (UMA) as one viable solution. Any policies discussed are illustrative and will vary by jurisdiction and business circumstances.

## 2. The Adolescent Use Case and Its Data Sharing Implications

This is a story about a young female patient named Julie Adams. We join her story when she is a young child. Her mother Sue Adams, acting as her legal guardian, is responsible for overseeing her health at this time.

Julie's pediatrician, Dr. Erica, provides a system for patients to securely share their data. While Julie is still a child, her mother manages and controls Julie's data. In Julie's state of residence, she is legally able to take control of her health data and make her own health decisions at the age of 14. This age policy varies by region, a situation discussed more in the section on [Policy](#), below.

Julie's story unfolds over several years, includes many health events, and involves many people:

- **Julie Adams:** female – starting as a child and becoming an adolescent
- **Sue Adams:** Julie's mother and legal guardian
- **Providers:**
  - Dr. Erica – Pediatrician
  - Dr. Robert – Asthma Specialist
  - Dr. Reynolds – Orthopedist

Julie experiences many events and encounters through her childhood. This report touches on the following:

- As a child, Julie's mother Sue finds her a Pediatrician, Dr. Erica.
  - A chart is started for Julie.
- Julie attends annual appointments with Dr. Erica.
  - Data is added to the chart for every appointment.
- At age 10, Julie is diagnosed with Asthma.
  - She visits an Asthma Specialist, Dr. Robert.
  - Dr. Robert needs access to Julie's health record to effectively provide care.
  - At the end of the appointment, he prescribes Julie an inhaler.
- At age 14, Julie is able to take a greater role in managing her health, including control of her clinical record and the ability to manage others' access to it.
  - Dr. Erica educates Julie on this new responsibility at her annual appointment.
- At age 16, Julie begins to experience sex and also begins using alcohol socially.
  - Julie does not feel comfortable discussing this with her mother, but does share this information with Dr. Erica in confidence during her annual visit.
  - Dr. Erica makes notes in Julie's record, provides relevant educational information, and discusses safe behavior, all as part of her overall evaluation for multiple potential risks of adolescents in transition.
  - During their discussion, Julie and her pediatrician agree she should be using an oral contraceptive and it is prescribed.
  - Julie is also tested for STI, which comes back positive.
  - Julie is prescribed Zithromax for the infection.
- Several months later, Julie breaks her wrist.
  - Dr. Erica sends her to an Orthopedist, Dr. Reynolds.
  - Julie wishes to keep her sensitive information from her previous encounters private.

Throughout Julie's journey, there are many events where health information is accessed by Julie or others, and where health IT could be used by Julie or Sue to enable more agency and participation. In addition, there are several policies that must be understood and enforced by both people and technical systems as Julie receives care and transitions between different health providers.

The following sections will expand on the complexity of health policy, introduce UMA and its strong support for FHIR, and ultimately show some ways an UMA-enabled ecosystem can improve Julie's care throughout her journey.

**Summary:** The “Adolescent” use case proposed by PP2PI involves many actors (patients, family members, healthcare providers) and changes in circumstances (health status, age, responsibility, privacy preferences). Key moments in the journey illustrate specific data-sharing requirements.

### 3. The Nuts and BOLTS of Policy and How It Impacts Julie's Journey

The term "policy" covers many different elements, including business, operational, legal, technical, and societal aspects. The identity industry has taken to calling this "BOLTS". These policy systems typically address liability, access control, compliance, patient transparency, and more. Touching on a few key examples:

- There is a robust regulatory landscape that defines how health systems must operate, for example, touching on security, privacy, covered entities, consumer protection, the Internet of medical things, and more.
- At the societal level, issues of public health, consent, anonymization, and clinical research arise.
- Businesses with different financial models and regimes come with a variety of oversight mechanisms and associated policy.
- Health data ecosystems often manage data sharing through bidirectional contracts or through "trust frameworks" that function as master service agreements.

Often the implementation of policy excludes the most important person: the patient who is the subject of the data being collected, used, and shared. Concerns about [information blocking](#) have led to signs of change. For example, the [21st Century Cures Act](#) is a law driving much current effort in the US to change the current patient-excluding dynamic by regulating that patients must have a simple way to access their information to their benefit.

Patients expect certain ways of experiencing and interacting with health systems, particularly in the era of Apple Health, which eases user-centric access to and sharing of health data. The self-service ability to set and view consents to share data, access history, and sharing policies can be viewed as a kind of policy along with all the others.

The new regulations make it clear that patient-mediated exchange is required in today's world. Organizations must find solutions for patient access to and exchange of their health data. There is an ever-growing number of real implementations where patients are put in control of their data, clearly showing that these outcomes are achievable.

**Summary:** Many layers of policy influence and determine aspects of health data sharing. Patients are key stakeholders in data access and sharing, a right now more strongly recognized in regulations. Patient data control is starting to become a reality in some IT systems, and the parameters of such control can be considered as a kind of policy that should be addressed along with the others.

### 4. Overview of UMA and HEART and Their Relationship to FHIR

The User-Managed Access (UMA) standard, and its companion Health Relationship Trust (HEART) profiles, address some key challenges related to digital data sharing, including health

data. These technologies work by enabling a patient to specify which of her records, and even partial data sets, she would like shared with other parties. In essence, it allows her to state her precise policies for data sharing and have those policies adhered to by the various service providers and applications handling her data.

The UMA standard can be used by people and systems to protect and share data of any type, as long as it comes from a web server and has some kind of API. It is designed to enable practical, secure, auditable sharing controls in ecosystems that may involve many services and applications.

The HEART profiles tune UMA for use with clinical health data use cases, ensuring security protection to a level appropriate for sensitive personal health data and providing instructions for interoperability with OpenID Connect, the FHIR API, various HL7 value sets, and the SMART on FHIR architecture.

Both UMA and HEART share a goal of empowering the person at the center of this picture: she is the "user" in User-Managed Access. One or both standards may be used to address some of the key data sharing challenges illustrated by PP2PI.

## Introducing the Actors in the Standard

In order to specify how they interact, UMA lays out a number of different actors, or "entities," in different communication roles. UMA is based on OAuth, the standard already used in SMART on FHIR, so it mostly uses entity names that come from OAuth.

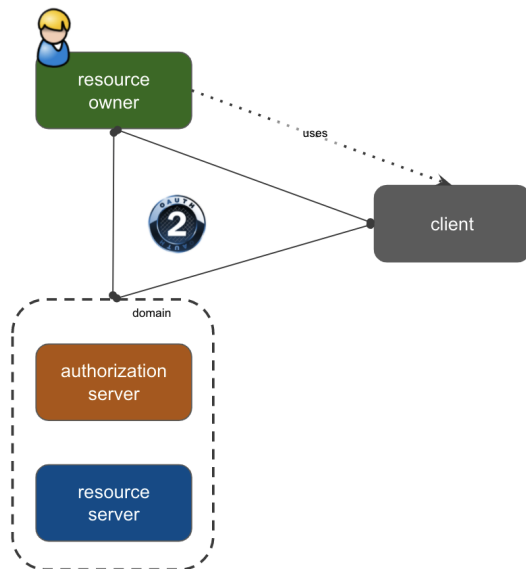
- **resource owner:** Normally the patient (or other data subject), or possibly a person who has special duties to act on her behalf in setting her sharing policies (for example, a legal guardian).
- **requesting party:** The person trying to get access to the data in question. When the resource owner specifies a sharing policy, she indicates her desired requesting parties as the target. This concept is unique to UMA.
- **client:** Stands for "client application," for example a mobile or web-based app that is FHIR-enabled and can be used by a specialist to attempt access to the data.
- **resource server:** The service provider hosting the data to be shared (or protected). A FHIR server is an example of a resource server.
- **authorization server:** A special kind of server whose job is to assess and mediate data access requests, on behalf of the resource owner.

**Summary:** The UMA standard enables personal control of data sharing with other people. The HEART profiles for UMA are standards that tune UMA for health-grade security and health data-specific use cases including the FHIR API and HL7 value sets. UMA is based on OAuth, which is used in SMART on FHIR, and the set of actors in the UMA protocol builds on OAuth.

## 5. OAuth and UMA

Let's look at how UMA builds on OAuth, already a key part of SMART on FHIR.

### General OAuth Background



OAuth enables a client application to request and receive a user's authorization to access some API service on her behalf. If the API enables many different actions, such as both reading and writing data, the authorization can be constrained or "scoped" to only some of the actions.

Every time the client attempts access to her data, it presents a "token" representing its authorization. The "token" lets the service check whether access is allowed without requiring the client to see the user's login information. The user can later revoke the token, withdrawing authorization.

OAuth represents a powerful improvement on previous ways of securing APIs, and a powerful end-user enablement method.

### OAuth in the Health Data Context

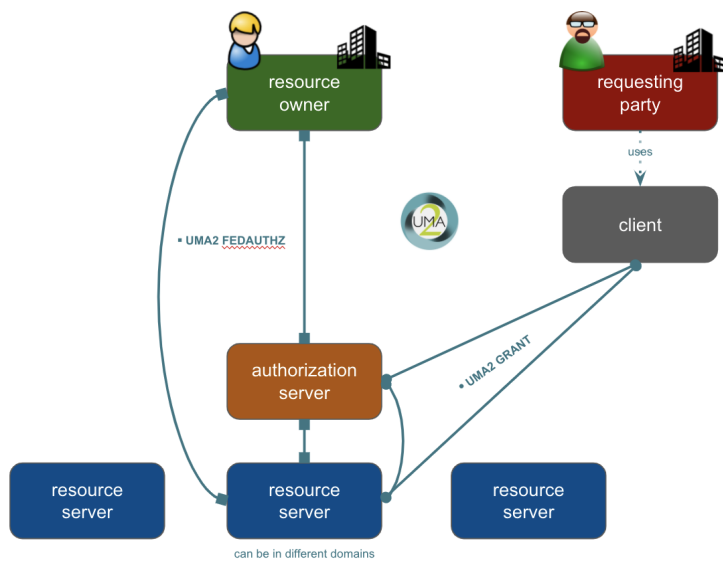
In healthcare, OAuth is primarily used for its API security benefits – not its user-centric features. Typically the scenario focuses on a healthcare provider using an application to access health data available at a FHIR API. Any data sharing wishes of the patient are handled outside the OAuth technology layer.

### UMA

While OAuth has one person in the picture, UMA has two, enabling sharing between them. Not only can the patient agree to access by an application that she uses; she can also specify ahead of time, or in response to a request, how a different person can gain access.

These two people don't have to be online at the same time. It's like the "Share" button in collaborative editing services like Google Docs. Unlike Google Docs, however, UMA also lets the user manage her sharing policies **across** multiple data sources.

UMA is related to OAuth in two ways.



First, UMA expresses how the requesting party and client app gain data access with a “grant”: an OAuth flow. The right half of the figure illustrates the **UMA grant**.

Second, UMA lets the user manage trust between her authorization server and multiple data servers, making a wide ecosystem of data servers possible. To protect the API it has defined for this, UMA simply uses OAuth in its traditional sense. The left half of the figure illustrates this **federated authorization** mechanism.

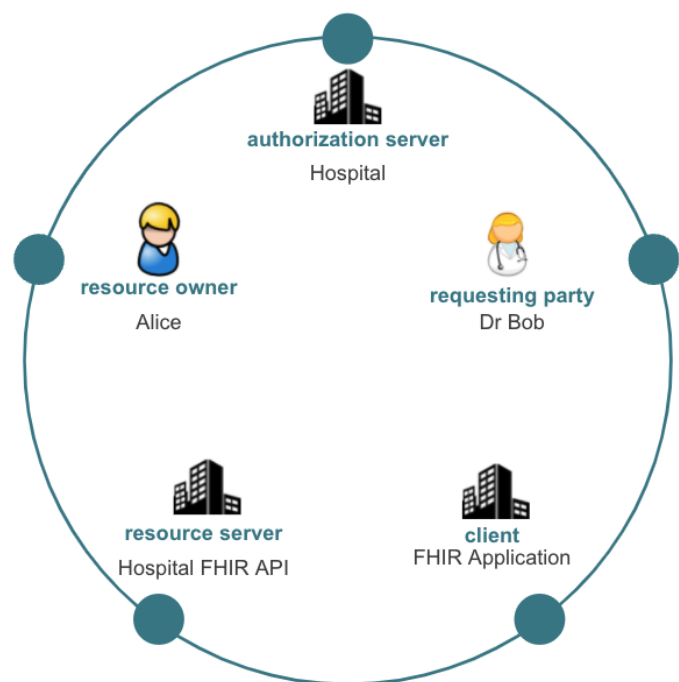
**Summary:** OAuth improves the interoperability and security of API protection, and empowers users to connect new apps to services they use. OAuth usage in the health data context puts an emphasis on API security rather than patient centricity. UMA builds on and leverages OAuth to enable powerful new scenarios for patient-centric data sharing.

## 6. Basic UMA Use Case

**Alice visits a hospital and has a few tests performed. She wants Dr Bob to be able to access some of the test results.**

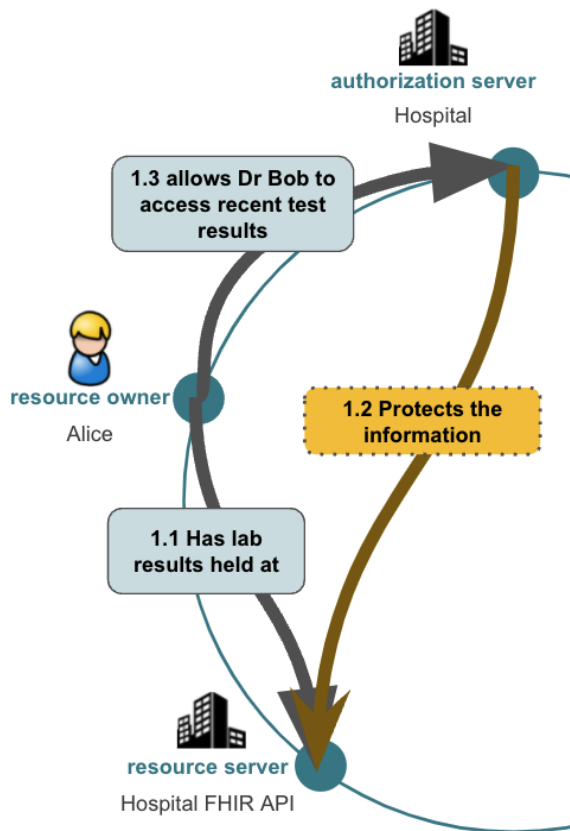
This straightforward use case immediately goes beyond the scope of a pure OAuth solution: the person accessing information is not the resource owner, the 'scope' of access is fine-grained to specific results in a wider set of all test results, and the resource and authorization servers need not be hosted by the same organization. *Please note, the actors in this section are unrelated to Julie and her story.*

**1.1, 1.2: The hospital holds Alice's information and results, available through a FHIR API. The hospital also**





provides an authorization server, where Alice's FHIR resources are registered for her.



The UMA flow starts with a resource owner's information held by a resource server. This information is available at different resource locations (eg urls). These resources are registered at an authorization server for the resource owner.

The authorization server can protect information from many resource servers, allowing a resource owner a single place to manage their information. Resources can be registered in broad or fine grained ways, from an entire FHIR API to a specific FHIR Observation. The resource server declares what resources it holds, and what scopes it can support to further define access - at the end of the flow, the resource server must be able to understand and enforce access to the information.

**1.3: Alice uses the authorization server to allow Dr Bob access to some of her recent test results held at this hospital. Alice shares the url of the results with Dr Bob**

The core sharing capability of UMA allows the resource owner to create policies at the authorization server, declaring the conditions that requesting parties must meet to access the specific resources. The authorization server can also create default policies, such as to always allow the owner access.

The conditions to access resources are specified by claims that must be presented by a requesting party. A single resource may have multiple different claims requirements. Claims may be as simple as “a doctor at organization ABC with an NPI of 12345” or “an ER physician at organization ABC with 'break the glass' access rights.”

### 2.1: Dr Bob puts the URL in his client, which then learns the authorization requirements. The client redirects Dr Bob to the authorization server

The requesting party uses some client software to access the information. The client accesses the location of the information (e.g. a url) at the resource server, and is directed to the right authorization server

The UMA client application can be very general since it doesn't need ahead of time knowledge of the authorization server or the scopes required to access the information. The resource server directly works with the authorization server to create a ticket representing the resources and scopes requested by the client. The client can follow the steps provided by the resource and authorizations servers to support many possible authorization flows.

### 2.2: Dr Bob is able to login using his usual credentials in this health network. The authorization server decides if the claims meet Alice's policy for the test results

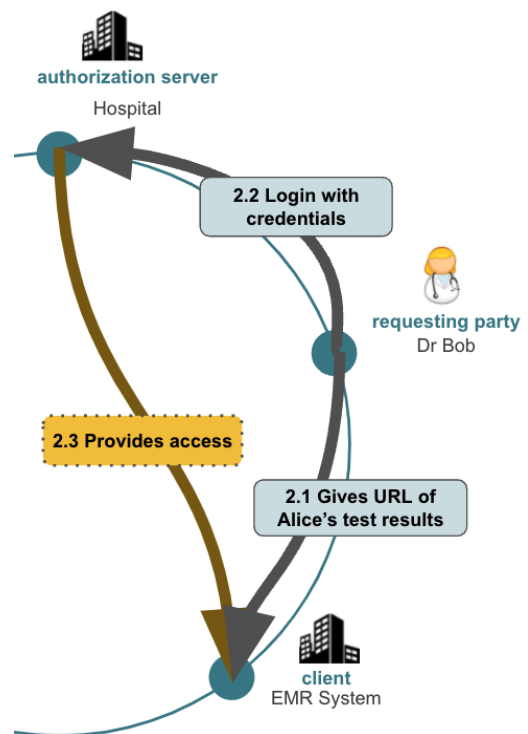
The requesting party is able to present claims to the authorization server. The claims are evaluated to see if they meet the conditions of the resource owner's policy,

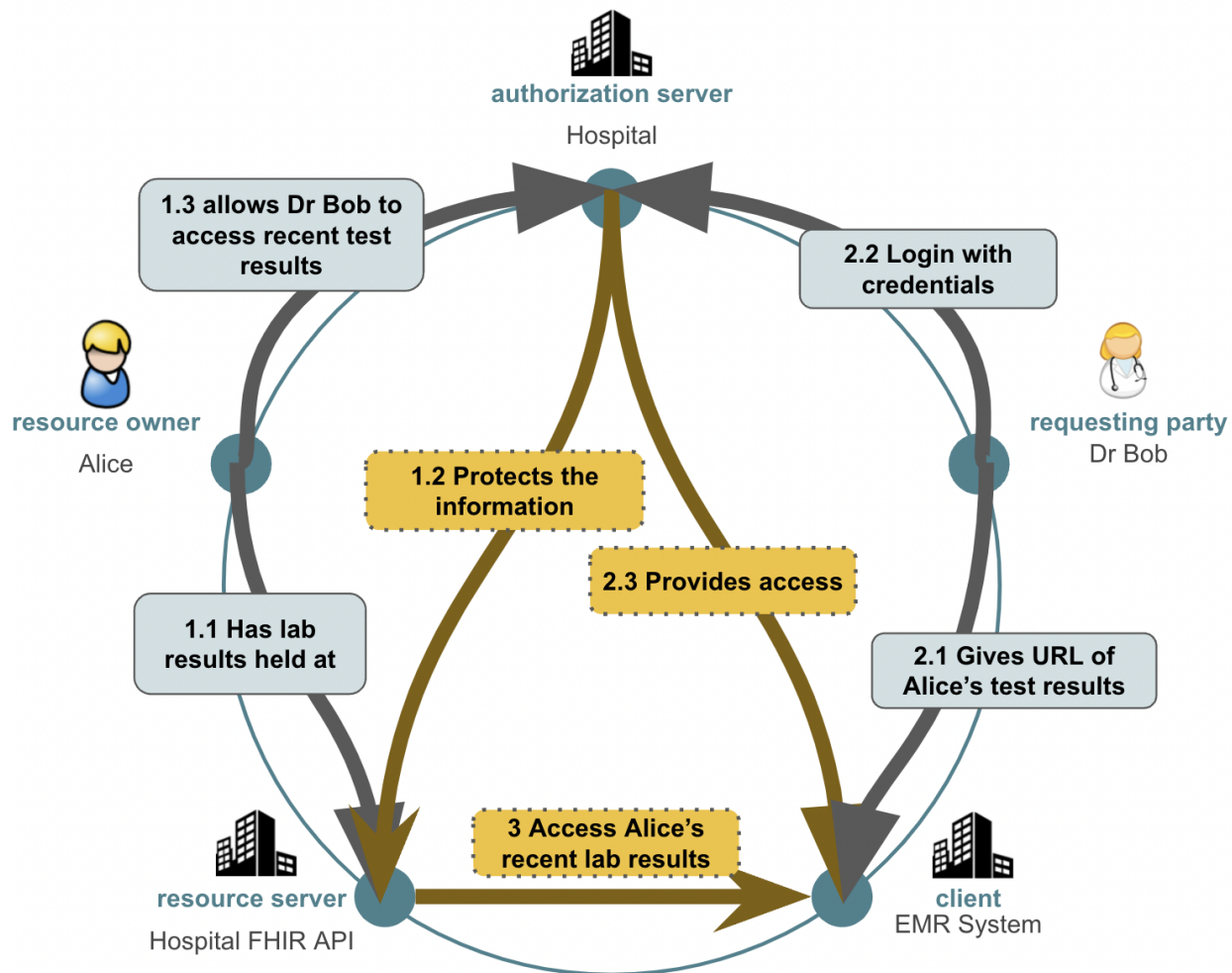
UMA is flexible about identity and how people authenticate. In a simple case, the authorization server itself acts as an identity provider for both resource owners and requesting parties. In more complex scenarios, the authorization server may federate to other identity providers, or allow the client to directly present claims it already holds for the requesting party.

### 2.3, 3: Dr Bob's client is able to receive Alice's specific test results from the hospital's FHIR API

If the authorization determines the claims presented meet the resource owners conditions, the client is issued an access token and the requesting party is allowed access to the information.

The resource owner does not need to be online when their resources are accessed. They are able to revisit the authorization server and view what access has taken place, and remove or modify existing policies, at their own convenience.





**Summary:** UMA's standardized interactions between actors enable a wider and more general data sharing ecosystem, allowing different parties to take part in data access-granting (the resource owner/access rights administrator), access-authorizing (the authorization server), access-enforcing (the resource server), and access-seeking (the requesting party and the application they use).

## 7. Delegating Control of Access Rights

So far, we have discussed how UMA enables **delegation of access** to online resources. Often, patient-mediated exchange is implemented to enable the patient to define *their own* policies for others' access to *their own* data. This scenario includes many use cases, with many benefits to both patients and healthcare systems.

UMA also frequently interacts with the concept of **delegation of control**. When a patient is not able to manage, or may not be interested in managing, their own data sharing policies, transferring or sharing control comes into play. For example:

- The patient is an infant or child and is not yet capable.
- The patient is elderly or is incapacitated in some way.
- The patient prefers – for example, because of ill health or lack of regular access to online systems – to choose a delegate to handle data access and sharing, such as their spouse, an adult child, or a care coordinator.

Under any of these conditions, the UMA framework and flows can be combined with additional policy, to enable delegating *control of access* to their health data, to someone else. This is sometimes known as delegated administration.

As illustrated below, there are four states of delegation of control. The two states in the first column represent cases where the patient is one of the parties able to manage their own resources, and the second column represents cases where users other than the patient are administering policy. The two states in the first row represent cases where there is a *single* individual controlling access, and the two states in the second row represent cases where *multiple* individuals control access.

	Data subject can manage own resources	Data subject cannot manage own resources
1 administrator	<b>Self-administration:</b> Competent data subject as self-representative	<b>Administration by proxy:</b> Single representative of ward
2 or more administrators	<b>Co-administration:</b> Multiple representatives of data subject, including self	<b>Co-administration by proxy:</b> Multiple representatives of ward

In a simple use case of self-administration, the patient is both the data subject and the administrator of their own resource rights. In more complex use cases, someone other than the patient may enter the picture as an administrator, and that role could also be shared among multiple parties.

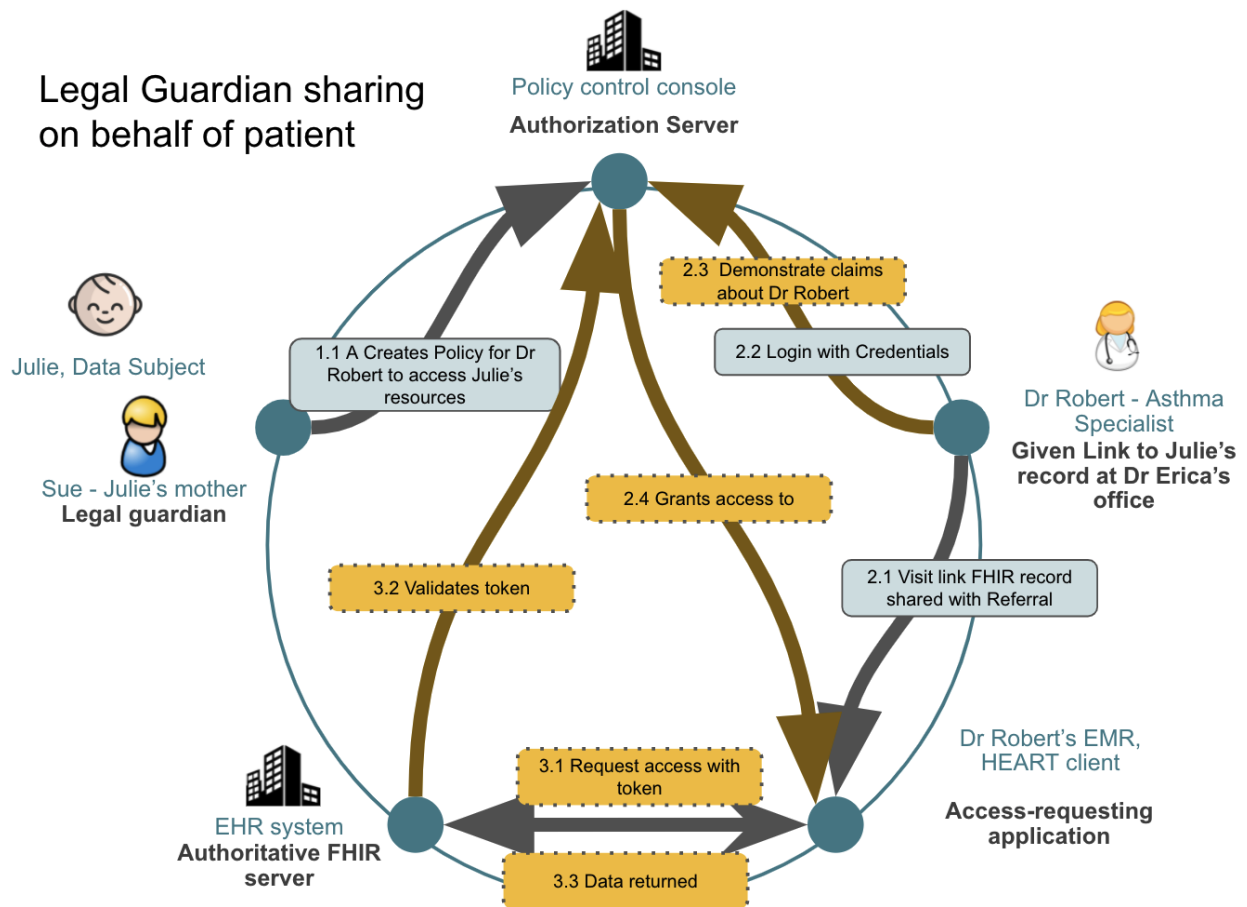
Whenever control is being delegated, it’s a critical moment. It can be thought of as a new **relationship** (such as proxy–ward) being formed, or a previous relationship being ended. A number of legal, operational, technical, etc. policies may apply to these junctures, ensuring the right parties are in the relationship and have the right characteristics.

**Summary:** UMA’s main purpose is to support data subjects’ ability to delegate access rights to their own data. Often, health data management also requires delegation of control of granting such access rights, sometimes called delegated administration. This enables others to assist those who are incapable of personally specifying the access rights, or who need help. UMA can be used along with additional layers of policy supporting this larger capability.

## 8. Applying UMA to Julie’s Story

Let’s go all the way back to Julie’s birth. In the jurisdiction where she was born, her parents or other legal guardians need to become administrators of baby Julie’s clinical data. Let’s assume that Julie’s mother, Sue Adams, is the sole legal guardian and therefore needs to be in charge of any sharing of Julie’s health data. The newborn and her mother are in the data sharing relationship **administration by proxy**. If Julie had two parents in this role, **co-administration by proxy** relationships would need to be set up instead.

At the age of 10, Julie is diagnosed with Asthma and will visit an asthma specialist, Dr. Robert. Dr. Robert needs access to Julie’s health record in order to effectively provide care. Julie’s mother, Sue, creates a policy to share all of Julie’s data with Dr. Robert. This flow is very similar to the earlier UMA flow demonstrated, with the difference that an administrator (legal guardian) is defining the policy instead of the patient defining the policy.



The steps are very similar to the basic UMA use case.

1.1. The legal guardian creates a policy to share Julie’s data with Dr. Robert.



- 2.1 Dr Robert is provided a link to access the data. He is redirected to the authorization server where
- 2.2 He logs in with his credentials.
- 2.3 As part of his authentication his claims are also validated.
- 2.4 The authorization server grants access to Julie’s data by providing a token.
- 3.1 The client requests access, this time with a token from the authorization server.
- 3.2 The resource server (FHIR API) validates the token with the authorization server, then
- 3.3 returns that data to the client.

**Summary:** The birth of the child triggers the delegation of access control, where the legal guardian has the right to administer the data access for the patient’s data. Later, the legal guardian shares data with the Asthma specialist on behalf of the patient.

## 9. Julie Begins Self-Administration of Her Clinical Data

At the age of 14 in the state where Julie lives, she is able to take a greater role in managing her health, including control of her data. At her annual appointment, Julie and Dr. Erica discuss this new responsibility, and Julie is educated on how to manage access to her clinical record.

Using the delegation of control framework, a new delegation state change is triggered. The state change from our earlier diagram moves from quadrant 1b to quadrant 1a, and the data subject, or patient, has control for data access to her own record. For our user story, Julie is now the resource rights administrator for her own data.

	Data subject can manage own resources	Data subject cannot manage own resources
1 administrator	<p><b>Self-administration</b></p>  <p>data subject now administrator 14 year old Julie</p>	<p><b>Administration by proxy</b></p>  <p>no longer administrator Julie’s mother, Sue</p>
2+ administrator	<p><b>Co-administration</b></p>	<p><b>Co-administration by proxy</b></p>

**Summary:** Due to a policy we have a state change of delegation of control. The patient, Julie, can now administer her own rights, and has control over her own data.

## 10. Julie's Record Collects More Sensitive Data as She Matures

When Julie is 16, she begins to experience sex and also begins using alcohol socially. Julie does not discuss this with her mother, but Julie does share this information with her pediatrician in confidence during her annual visit. Her pediatrician discusses these details with Julie and makes notes in her record. Her pediatrician provides relevant educational information and discusses safe behavior, as part of her overall evaluation for multiple potential risks of adolescents in transition. During their discussion, Julie and Dr. Erica agree she should be using an oral contraceptive and it is prescribed. Julie is also tested for STI, which comes back positive. Julie is prescribed Zithromax to clear the infection.

As part of growing up, Julie begins to keep some personal information private.

**Summary:** Julie develops sensitive conditions which are recorded in her health record.

## 11. Granular Sharing of Julie's Data Using UMA and HEART

Several months later, Julie breaks her wrist. Dr. Erica sends her to an orthopedist, who is a friend of Julie's family. Julie has not previously seen Dr. Reynolds, the orthopedist, so it is very helpful to provide her complete clinical record in advance of the visit. Julie wants to share her data with the orthopedist but wishes to keep her sensitive information private.

When Julie creates her policy to share clinical data with her orthopedist, she requests that her sexuality and reproductive health information not be shared. (More specifically, when Dr. Reynolds requests her clinical data, her sensitive data around sexuality and reproductive health be excluded before sending that on to Dr. Reynolds.) That is all the patient needs to do, the rest is handled by the exchange system.

When her orthopedist, Dr. Reynolds, accesses her data, based on the computable consent created by Julie, any clinical data that has 'sexual and reproductive health' information sensitivity will be redacted before it is sent to Dr. Reynolds.

The system Julie is using to share her data is based on FHIR and UMA/HEART and supports data segmentation for privacy.

At the resource server level, the data is 'tagged', indicating what elements fall into the sensitive data around sexuality and reproductive health information. This is typically an automatic process occurring in the FHIR server. A tagging engine would run Julie's data against a value set terminology to determine what if any of her clinical data is sensitive.

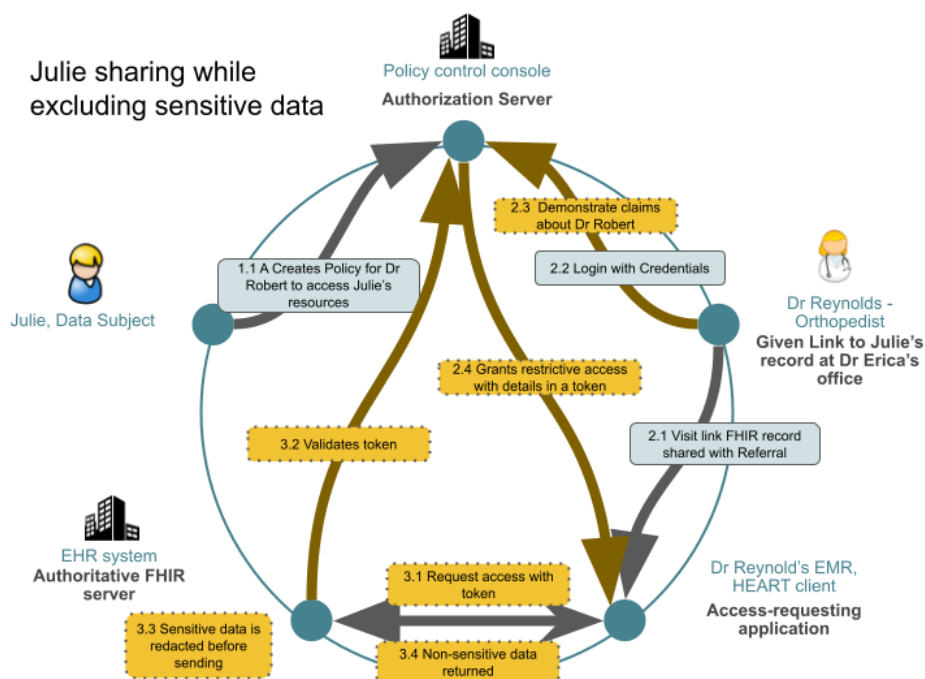
For Julie's case, the following two areas of her clinical data would be marked sensitive:

- Condition for STI – which is no longer active (sens/STD) - Sexually transmitted disease

- Prescription (Medication) for Oral Contraceptives (sens/SEX) - Sexuality and reproductive health

Each of these would be recognized by the tagging engine and the metadata would carry the indicated code as shown in the parenthesis.

As the HEART client makes a FHIR request, the FHIR server uses the access token to determine at a granular level what data to include or filter from it's response. Only properly authorized data will be shared. When the payload is created to send back to the client, any data tagged as sensitive for STD or SEX will be redacted.



18

The steps are very similar to other UMA use cases, with the addition of the HEART profiles to support sensitive data.

1.1. This time Julie creates a policy to share her data with Dr. Reynolds.

2.1 Dr Reynolds is provided a link to access the data. He is redirected to the authorization server where

2.2 he logs in with his credentials.

2.3 As part of his authentication his claims are also validated.

2.4 The authorization server interprets Julie's policy (consent) for sharing with Dr Reynolds. When the authorization token is created, additional detail is added indicating that the sensitive data should not be shared.



- 3.1 The client requests access again, this time with a token from the authorization server.
- 3.2 The resource server (FHIR API) validates the token with the authorization server.
- 3.3 When the data is prepared, any data that is either STD or SEX sensitive is redacted from the data to be returned.
- 3.4 Returns non-sensitive data to the client.

Break the Glass functionality can be supported by combining claims with either a patient or organizational policy, allowing emergency access to data not explicitly shared.

**Summary:** The user interface and process is easy and intuitive. Patients have the right to share data at a granular level and are provided options to make those choices where appropriate. Using UMA and HEART, data is securely delivered to the requesting party while honoring patient privacy and security.

## 12. Conclusion

This report demonstrates three key themes:

- **Patient-centric data sharing** in our complex health IT world benefits from technology solutions that address these new challenges and which do more than the OAuth technology we have today.
- **UMA** complements and builds on previous solutions, adding unique value to the patient-centric data sharing equation.
- **Real-world relationships** are an integral element of any patient-centric data sharing solution. The UMA framework for delegation of access, combined with identity assurance and claims, all contribute to a robust solution.

Technology is no longer the problem in solving Julie Adam's data sharing challenges. Policy definition is still difficult, and requires a wide range of inputs. However, once policy is defined, we have the tools to implement it securely. A crucial element of policy is the consideration and inclusion of the patient's wishes. UMA is designed to include the patient in the definition, execution, and maintenance of policy – enabling Julie to meaningfully participate in a patient-centric data sharing ecosystem.

## A. PP2PI Scenario Assumptions and Simplifications

For the purposes of this report, we have intentionally simplified the PP2PI Adolescent scenario to focus on UMA's key value-adds in solving this problem. For this report, we took the liberty of organizing the story so that we could build on the UMA/delegation functionality to improve the story flow.

We have made the following changes and assumptions:

- The PP2PI story focuses on Julie's own access through a portal. We broadened the story to assume that the health data could be in any repository that allows the patient to control access (patient-mediated exchange).
  - We also address the broader use case where individuals beyond Julie have access. UMA could certainly be used for portal access as well.
- There may be some states where a parent and their child have different levels of data access. For simplicity, we assumed a parent's administration rights would transfer completely to the data subject when she reaches a certain age.
- We illustrate patient policy only, but in fact, most UMA implementations combine some level of additional policy with patient-defined policy.
- The ages used here reflect the policies in effect in the state where the scenario takes place. The correct age restrictions for other jurisdictions can be substituted.
- We illustrate using UMA only to control patient-to-provider data access. It can also be used to share data with many types of organizations (public health, research, etc.) and individuals acting on their own behalf.

We have omitted the following details because they are out of scope:

- We do not describe how labs, pharmacies, or payers manage sharing of sensitive data. UMA could be used to help these organizations. It is a best practice to have policies in place to eliminate risks in these circumstances. For example, a pharmacy might call to say a prescription is ready but should not reveal what the prescription is for to anyone but the patient. Edge cases in these circumstances need to be defined by other PP2PI workgroups.
- We treated non-technological policy and ethical considerations as out of scope for this paper. The PP2PI policy/ethics workgroup is addressing elements here.
- We treated the question of not sharing all clinical data with a clinical provider as out of scope. There are sensitivities and tensions around this question that go beyond the technical.

## B. About This Report and the Standards Mentioned

This report is produced by the [User-Managed Access \(UMA\) Work Group](#) of the [Kantara Initiative](#). As this report focuses on using UMA in the healthcare sector, it touches on several health IT-related standards and efforts.

UMA is an award-winning OAuth-based protocol designed to give an individual a unified control point for authorizing who and what can get access to their digital data, content, and services, no matter where all those things live.

Kantara Initiative, Inc. is an international ethics-based, mission-led nonprofit industry “commons” focusing on growing and fulfilling the market for trustworthy use of identity and personal data.

The [Health Relationship Trust \(HEART\) Working Group](#) of the [OpenID Foundation](#) has defined several profiles that enable patients to control how, when, and with whom their clinical data is shared. These profiles are based on [OAuth](#), [OpenID Connect](#), and UMA. Several members of the UMA Work Group were also active in the effort to define the HEART profiles.

The [Protecting Privacy to Promote Interoperability \(PP2PI\) Workgroup](#) "is a national multidisciplinary interest group of expert stakeholders across the industry assembled to address the problem of how to granularly share clinical data to protect patient privacy and promote interoperability and care equity." It develops use cases, provides implementation guidance, and works towards adoption.

Although some members of the UMA Work Group take part in the PP2PI effort as well, this report has no formal relationship with PP2PI. We seek feedback from PP2PI and others on this report.

This report also mentions several key healthcare-related open API standards and technologies, including HL7's [FHIR](#) API and resources, and [SMART on FHIR](#).

## C. Other Related Technologies

Implementers of UMA and HEART tend to integrate them with the following key technologies and concepts.

### **Federated Identity and Identity Assurance**

UMA works hand in hand with strong identification and authentication. We strongly advocate supporting [NIST Special Publication 800-63](#), which defines standard levels of identity, authentication, and federation assurance.

### **Consent Receipts**

Patients have a right to know what consents they have created and to modify and revoke existing consents. The Kantara Initiative [Advanced Notice & Consent Receipts Work Group](#) defines standards and processes for generating such proof.