# ­­Problem Statement

Alice, a stage 4 cancer patient, is registered with a PCP, oncologist, local hospital system, outpatient laboratory, outpatient radiology imaging, and a retail pharmacy chain. She has two-way agreements to send and receive data from each health provider’s EHR and her PHR. (See HEART Use Case: Alice Registers with PCP and Sets Up Two-Way Exchange of Personal Data Between EHR and PHR [OAuth Only].)

Alice has also granted her son access to her PHR, along with the ability to act as her health care proxy. This is done out-of-band for this use case. (See HEART Use Case: Elderly Mom with Family Caregiver.)

Given a dismal prognosis, her oncologist has recommended that she enter a clinical research “basket study” for a genomic-informed selection of chemotherapeutic agents. This will include a biopsy sample of her cancer, stored for current and future research, and genetic sequencing for specific oncogenes. The clinical researcher will have access to her entire aggregated clinical record and PHR in addition to genomic and pathology data from the biopsy.

After reading the overview of the clinical research and the disclosure of privacy practices for the study, in concert with her son, she grants consent for the study via her oncologist’s EHR system. As part of this consent, remembering the infamous case of Henrietta Lacks, Alice wants to preserve her right, and that of her heirs, to monitor clinical researchers’ access to her data and to revoke consent.

Subsequently, the clinical study administrators register for access to her clinical data residing in each health provider’s EHR system as well as Alice’s PHR. This is done out-of-band to this use case.

In order to aggregate the clinical data, the clinical study has a database system that gathers clinical data from the health providers’ EHRs. Clinical researchers access the aggregated data.

Upon analysis of the data, the clinical researchers select a chemotherapeutic agent to be used for Alice. They inform the oncologist of this choice, via the EHR. As treatment progresses they monitor new data collected about Alice. They construct a longitudinal aggregate record from this. Every access to Alice’s data is recorded, with a summary sent to Alice’s PHR.

Unfortunately, Alice succumbs to her cancer in six months. However, the accumulated clinical research record is available for subsequent use in a meta-analysis. The data are pseudonymized, masking Alice’s identity but enabling access to it if specific criteria are met.

A few years later, Alice’s son reviews her PHR and notes that a clinical trial has begun and is using information from the meta-analysis. The potential economic value of the cancer therapy is very high, so he contacts the pharmaceutical company and says he will withdraw consent unless Alice’s estate gets a share of the profits. Knowing that revocation will remove data and invalidate the statistical integrity of the meta-analysis, they offer a perpetual continuing access agreement in return for a share of the profits. Alice’s son signs it, and the pharmaceutical company enters it into the aggregate data, and informs the various EHRs and Alice’s PHR.

This use case addresses the following problems/issues:

* A patient’s informed consent for clinical research
* Secure and privacy-protected aggregation of clinical data from multiple sources.
* Secure and privacy-protected access to aggregate clinical data.
* Modification of consent for access to aggregated clinical data.

# Setup

Where this use case reflects a choice intended to inform the HEART WG’s profiling deliverables that may vary against use cases that reflect other choices, the notation **[CHOICE: *description*]** appears. This choice should appear in the title of the use case in brackets to help distinguish it from other close variants.

Where this use case reflects a discussion point for the HEART WG’s profiling efforts, the notation **[PROFILING]** appears.

Where this use case contains detail that is believed to be peripheral to the HEART WG’s profiling deliverables, the notation **[PERIPHERAL]** appears. The point of this detail is to give real-life “color” to the use case.

Relationship between the EHR-PHR parties is bound by previous arrangement (they know about each other) and are part of a trust framework.

## Ecosystem parties

* Alice: an individual; a patient who consumes healthcare services and participates in shared decision making regarding her care.
* Alice’s son: an individual who Alice has granted rights of access equal to her own and whose rights persist after Alice’s death.
* Personal health record (PHR) system operator: a provider of a PHR system, a private Internet-facing information system that tracks Alice’s medical information for her where Alice is the end user with authority over her data, and where the PHR system operator supports many such end users. This document uses “PHR” exclusively to refer to a “patient-controlled” or “untethered” type of PHR to avoid confusion.
* Care providers (CPs): health care professionals who see Alice during the course of her treatment; end users of electronic health record (EHR) enterprise Internet-facing information systems that track many patients’ medical information, and have a patient-facing portals. This document uses “portal” exclusively to refer to a “tethered” type of PHR to avoid confusion. CPs may share data among themselves, via EHRs or otherwise, but that is outside this use case’s scope.
* Data Aggregation system operator: the provider of a system that gathers and aggregates patient data from the Alice’s PHR and the EHRs of her CPs, plus the same data for other patients. The system also aggregates disclosure records to track access to patients’ data, periodically reporting the disclosures to the patients’ PHRs.
* Clinical Researchers: people who access the Data Aggregation system to inform their clinical research.
* Institutional Review Boards: committees of people who ensure that clinical research conforms to regulatory and ethical requirements. They issue authorizations to Clinical Researchers to perform the research and access the Data Aggregation System. They also issue authorizations to the Data Aggregation system operators to gather the patients’ data.

## Technical preconditions

* Network facilities exist to provide sufficient administrative, physical, and technical mitigations to security risks to computing systems’ and data’s confidentiality, integrity, and availability. This is governed by service-level agreements that are out of scope to this use case.
* The PHR, EHRs, and Data Aggregation systems all use the standard FHIR API as their common interface.
* Clinical Researchers’ access is via a standard API that uses FHIR or that may be defined separately from HL7 FHIR.
* The PHR and EHR use OAuth to authorize access to the CPs APIs and the patient portals.
* The Data Aggregation uses UMA to enforce patient privacy policies for access to the PHR, EHR, and Clinical Researchers APIs.
* The patient privacy policies have a [standardized] computable vocabulary that is mapped to the FHIR and Data Aggregation APIs’ data resources.
* Pre-existing authorizations:
  + Alice’s PHR has a two-way relationship with her caregivers’ EHRs, as described in HEART Use Case: Alice Registers with PCP and Sets Up Two-Way Exchange of Personal Data Between EHR and PHR [OAuth Only].
  + The Data Aggregation system has read-only access to the EHRs, as authorized by the IRBs.
  + The Clinical Researchers have read-only access to the Data Aggregation system, as authorized by the IRBs.
  + The Clinical Researchers’ treatment protocols have been communicated out-of-band to the CPs. They are out of scope to this use case.
* Alice’s and her son’s access to the PHR is as specified in the HEART Use Case: Elderly Mom with Family Caregiver.

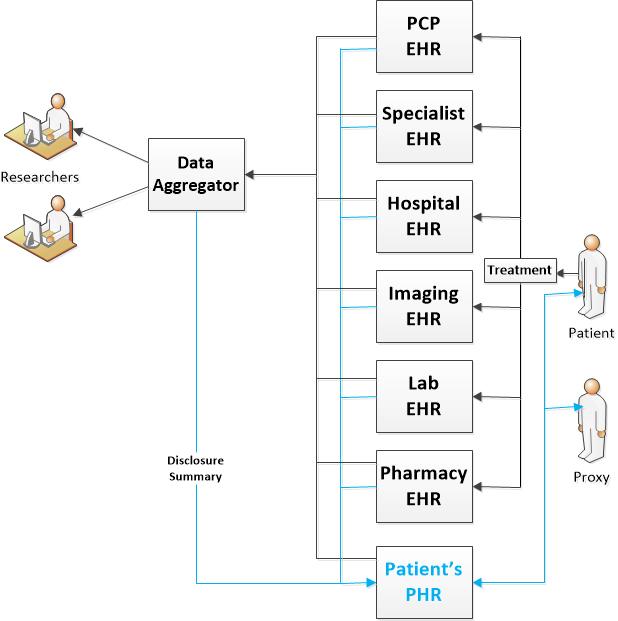
## OAuth and UMA entity roles

* Protected resource (PR): Online information or API that is access controlled through OAuth. Note that APIs can allow both “consumption of data” (read operations) and “insertion of data” (write operations) by authorized entities.
* Resource owner (RO): An entity that has OAuth access control rights to an online resource. The RO may not, however, have other “ownership” rights, such as the right to change data values within that resource.
* Authorization server (AS): An entity that issues OAuth access tokens representing the client’s authorization for access on behalf of the RO.
* Resource server (RS): An entity where the PR resides. In OAuth, the AS and RS are typically “tightly coupled” and run by the same organization (by contrast, in UMA, entities with these names might not be).
* Client: A web or mobile application (or even an IoT device) used by the RO that seeks and gains access tokens from the AS in order to access the PR. Access may be limited scoped) to a subset of possible API operations. The RO can typically visit the AS anytime to revoke the token.

## Party-to-entity mappings

**Data Flows**

* Clinical data as a result of patient treatment, to the various CPs’ EHRs.
* Clinical results data from the CPs’ EHRs to the patient’s EHR.
* Clinical research data from the CPs’ EHRs and the patient’s EHR to the Data Aggregator
* Disclosure summaries from the Data Aggregator to the patient’s PHR, then to the patient



**OAuth Flow**

*Drawing should show OAuth use, per PHR-to-EHR use case, for all EHR and the PHR.*

**UMA Flow**

*Drawing should show:*

1. *Consent from patient flowing from RO (patient), through oncologist’s EHR (or PHR?), to AS.*
2. *Request for access from Client (Data Aggregator) to AS for access to PRs at RSs (EHRs and PHR).*
3. *Access token returned to Client (Data Aggregator).*
4. *Client (Data Aggregator) gathers data from PRs at RSs (EHRs and PHR), as authorized by access token.*
5. *[optional] Modification of consent from RO (patient or proxy), through PHR, to AS.*

# Use Case Steps

## Patient Consents to Clinical Research

1. CP (oncologist) suggests that RO (patient) should consent to participating in a clinical research, allowing her clinical results data and PHR to be aggregated for research.
2. RO, after reading the literature about the test and the consent form, adds a condition that the consent may be withdrawn later, and signs it.
3. CP enters the consent data, plus a scanned copy of the signed form, into the EHR.
4. The EHR sends the authorization to the AS and to the PHR

## Clinical Researcher Accesses Data

1. The clinical researcher submits the research proposal to the IRB.
2. The IRB approves the proposal and sends an authorization to the AS for the client (Data Aggregator) to access the PRs at RSs (EHRs and PHR). This authorization restricts PR access to specific data that is needed for research
3. Client (Data Aggregator) asks AS for an access token to the PRs (EHRs and PHR).
4. AS processes the request, applying the RO (patient) authorization and IRB restrictions, grants access to specific data in the PRs (EHRs and PHR).
5. Client (Data Aggregator) accesses the PRs (EHRs and PHR), creating a local copy of the authorized data.
6. Client (Data Aggregator) creates a disclosure record and forwards it to the PHR.
7. Clinical researchers sign-on to the Client (Data Aggregator) - method and actions performed are out of scope.

## Patient Proxy Modifies Consent Provision

1. RO (patient) accesses PR (PHR) and views disclosure records.
2. RO (patient) accesses PR (PHR) and modifies the authorization, disallowing future access.
3. PHR forwards the modified authorization to the AS.
4. Subsequent requests by the client for an access tokens to the PRs (EHRs and PHR) are refused.­