Use Case: Alice Consents to Clinical Research [UMA]

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. The data will be available for additional clinical research. It will be pseudonymized, i.e., it does not identify her but can be reidentified under conditions specific to her treatment.

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, according to their Institutional Review Board policies, 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.

The operation of the clinical research network follows the conceptual network pattern of PCORnet.[1] To aggregate the clinical data, the clinical study has Clinical Data Research Network (CDRN) systems that gather 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 out-of-band. The oncologist enters the treatment protocol and medication orders that are, in turn, recorded in the EHR. As treatment

[1] See http://pcornet.org/

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.

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.

Use Case: Alice Consents to Clinical Research [UMA]

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. In a clinical research study there are many patients, and Alice is representative of them
- Alice's son: an individual who Alice has granted rights of access equal to her own and whose rights persist after Alice's death. There may be more than one rights grantee per patient, and each rights grantee may have similar rights for multiple study patients.
- 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. For this use case each patient will have one and only one PHR.
- 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. The CPs apply pseudonymization[2] to the data sent to CDRNs to de-idenitfy it for the purposes of research. CPs may also share data among themselves, via EHRs or otherwise, but that is outside this use case's scope. Each patient will have one or more CP, and each CP may have one or more patients.

[2] See *ISO/TS 25237:2008 Health informatics—Pseudonymization*, *IHE IT Infrastructure Handbook- De-Identification*, *and Algorithm Mapping Spreadsheet for use with handbook*

Use Case: Alice Consents to Clinical Research [UMA]

- CDRN system operators: the providers of systems that gather 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. There may be more than one CDRN used by the Clinical Researchers, and multiple clinical researchers may access each CP.
- Reidentification system operators (RIs): the providers of services that can re-identify the pseudonymized[2] data in a CDRN for permitted purposes. In this use case the only permitted purpose is to send disclosure notices to the patient's PHR. There may be more than one RI, but only one participates in this use case.
- Clinical Researchers: people who access the CDRN systems to inform their clinical research, subject to IRB policy. If there are multiple CDRNs, Clinical Researchers may create locally combined data aggregations with local access control, e.g., OAuth. There may be more than one Clinical Researcher accessing each CDRN, and each Clinical Researcher may access multiple CDRNs..
- Institutional Review Boards(IRB): 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 CRDNs. They also issue authorizations to the CDRN system operators to gather the patients' data. Although there are multiple IRBs, this use case assumes only one IRB for each clinical research study.
- Authorization Service: an entity that stores IRB authorization data for granting ecosystem parties access to patient data. This use case assumes only one authorization service for each IRB.

Business Preconditions

- Patients have a trust relationship with their care providers and PHR. This is evidenced by regulation-mandated documentation.
- Patients may have trust relationships with relatives, with defined authorities to view clinical data and to act on their relative's behalf. This authority may extend beyond a patient's death. It is evidenced by legally-mandated documentation.
- There are formal written agreements that record these preconditions:
  - Data-sharing trust relationships exist among the participating provider organizations, the CDRNs, reidentification system operators, and the clinical research IRB. The IRB ensures all of this is in compliance with all applicable federal, state, local, and institutional data security and privacy policies.
  - The patients' consents for research create a trust relationship among the patients' PHRs, the CDRNs, and the clinical research IRB. The IRB ensures this is in compliance with all applicable federal, state, local, and institutional data security and privacy policies.
  - The clinical research IRB has a trust relationship with an authorization service.

Use Case: Alice Consents to Clinical Research [UMA]

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 research data network exists and follows the PCORnet conceptual pattern.
- The PHR, EHRs, and CDRN systems all use the standard FHIR API as their common interface. **[peripheral]**
- Clinical Researchers' access is via a standard API that uses the PCORnet Common Data Model. **[peripheral]**
- The PHR and EHR use OAuth and/or UMA, with scopes as defined initially by SMART on FHIR, to authorize access to the CPs APIs and the patient portals. **[core]**
- The CDRNs use UMA to enforce patient privacy policies for access to the PHR, EHR, and Clinical Researchers APIs. **[core]**
- The patient privacy policies are pre-coordinated with the EHRs and PHR so that the clinical research authorization token restricts query responses to pseudonymized data sets containing only the elements pertinent to the clinical research.
- 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 CDRNs have read-only access to the EHRs, as authorized by the IRBs.
  - The Clinical Researchers have read-only access to the CDRNs, 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.

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..
- **Requesting party** (RqP): An entity that seeks access to a PR. May or may not be the same party as the RO.
- **Requesting party token** (RPT): An UMA access token.
- **Authorization server** (AS): An entity that issues RPTs representing the authorization of the client and the RqP operating it for access. There may be more than on AS within the

technical ecosystem, but only one is associated with the clinical research and it is the sole source of authorization data for all patient data access for the clinical research study.

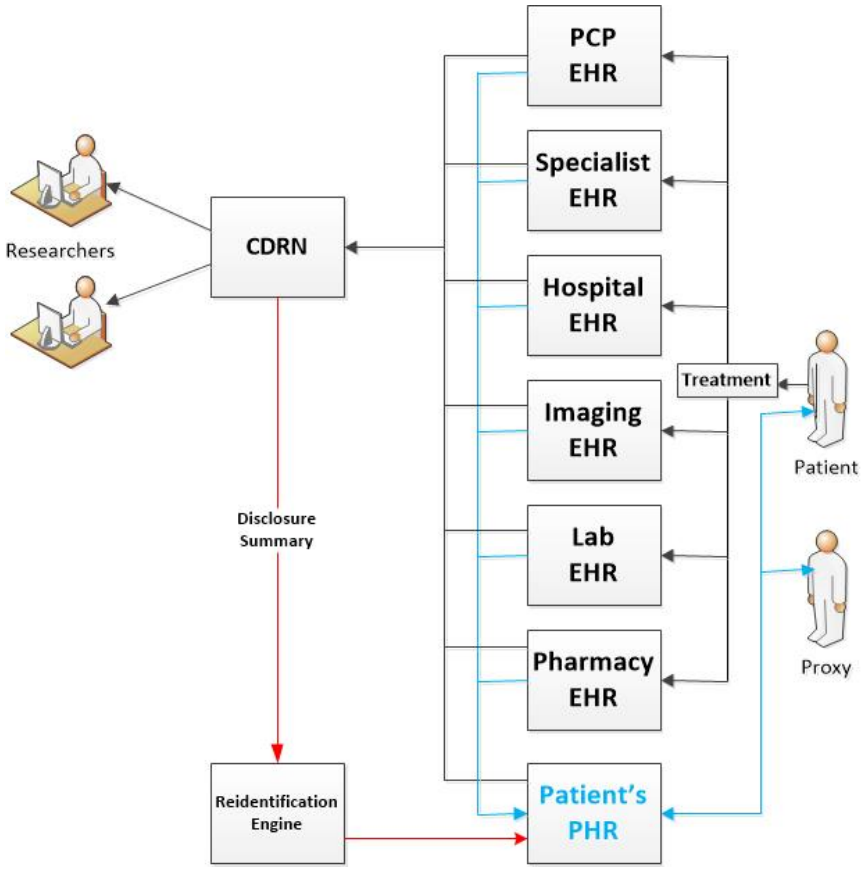
- **Resource server** (RS): An entity where the PR resides. The AS and RS can be “loosely coupled” and run by different organizations or entities, enabling the centralization of multi-RS management, fine-grained authorization modification, and RO choice of AS.
- **Client**: A web or mobile application (or even an IoT device) used by the RqP that seeks and gains RPTs from the AS in order to access the PR. Access may be limited (scoped) to a subset of possible resource sets and API operations on them.

Use Case: Alice Consents to Clinical Research [UMA]

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 CDRN
- Disclosure summaries from the CDRN to the patient's PHR, then to the patient



Use Case: Alice Consents to Clinical Research [UMA]

Use Case Steps

Clinical Research Set-up (preconditions)

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 CDRN to access the PRs at RSs (EHRs and PHR). This authorization restricts PR access to specific data that is needed for research
3. RSs and CDRNs are provisioned with necessary data=handling and transformation tools.

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 by CDRNs 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 clinical research AS and a record of it to the PHR

Clinical Researcher Accesses Data

1. CDRN asks AS for an access token to the PRs.
2. AS processes the request, applying the RO (patient) authorization and IRB restrictions, grants access to specific data in the PRs.
3. CDRN accesses the PRs, creating a local copy of the authorized data.
4. PRs create disclosure records for the CDRN access and forwards them to the PHR.
5. Clinical researchers sign-on to the CDRN - method and actions performed are out of scope, but OpenID and OAuth are recommended for consistency of security assurance.
6. CDRN creates a disclosure record for the clinical researchers' access and forwards them to the PHR, via the re-identification engine that converts the pseudonymization identifier to the actual patient identifier.

Patient (or Proxy) Modifies Consent Provision

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

Use Case: Alice Consents to Clinical Research [UMA]

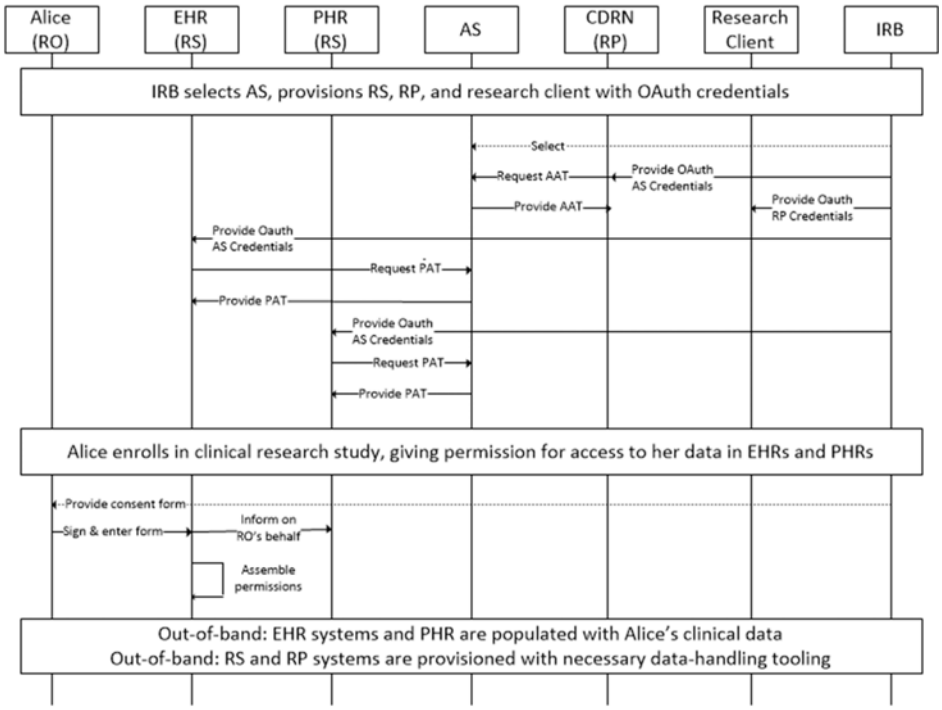
Sequence Diagrams

Note that the underlying message content conforms with the UMA profile for HEART.

Commented [GM1]: What is the correct reference for this?

Clinical Research Set-up

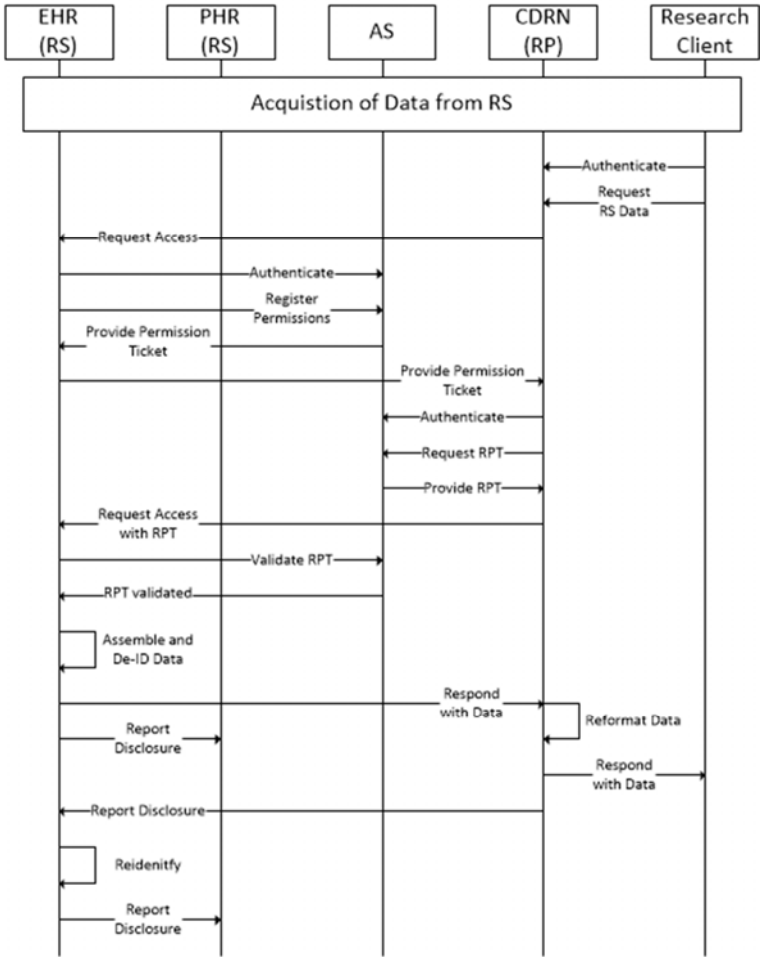
Note: "EHR" represents all RSs that may contain Alice's data.



Use Case: Alice Consents to Clinical Research [UMA]

Clinical Research Data Collection and Use

Note: Patient re-identification for disclosures reported by CDRN is done within the EHR



Use Case: Alice Consents to Clinical Research [UMA]

Review of Disclosures and Modification of Consent