Use Cases
for
Argonaut Project

Version 1.0

May 26, 2015

Introduction

The Argonaut Project seeks to rapidly develop a first-generation FHIR-based API and Core Data Services specification, along with a Security Implementation Guide, that together will facilitate expanded sharing of electronic health information. Our goal is to enable interested vendors and providers to develop and implement a focused but complete FHIR API specification, and accompanying security implementation, beginning in the spring of 2015. We recognize that the these specifications will introduce a new architectural pattern and style for accessing data and services, as well as new, more flexible and open, methods for authorizing access to health information. Therefore, we are proposing use cases that are simple, yet functional, and that address both real security risks and trust risks associated with potential discomfort with these new ways of doing things, as both of these can impede vendor and provider adoption.

We propose the following four functional use cases, as described below:

1. Patient uses provider-approved web application to access health data
2. Patient uses provider-approved mobile app to access health data
3. Clinician uses provider-approved web application to access health data
4. Clinician uses provider-approved mobile app to access health data

In addition, we have defined as a "near future" use case:

5. Clinician in organization A uses EHR A to access patient data in EHR B, operated by organization B

Definitions

EHR System: We use "EHR" in a broad context inclusive of any system that holds and controls individually identifiable health information. Each EHR system has the capability to mediate app requests for access and to authorize access to FHIR resources.

Provider Organization: We use the term "provider organization" to refer to any organization that holds individually identifiable health information.

Provider Approved: By the term "provider-approved" we mean that the primary data holder has developed, selected, or otherwise approved a named application as acceptable for enabling a user to access protected resources. The means by which that approval is accomplished are outside the scope of these use cases.

Mobile Application: By the term "mobile application" we include all applications that are hosted in environments that are incapable of providing assured protection of secrets. This includes applications that are downloaded and installed on mobile devices (e.g., iOS, Android) as well as rich web applications implemented within browsers. Mobile

applications essentially are applications hosted in any environment that lacks hardware segmentation of memory for isolating and protecting critical and sensitive code.

Web Application: By the term "web application" we mean an application that is hosted on a trusted web server and that is accessed through a user's web browser. A web application may be launched from a portal or EHR, or may be accessed directly through its URL. A web application is capable of protecting a secret assigned to it to for use in authenticating its own identity.

Use Case 1: Patient uses a provider-approved web application to access health data

Introduction

In this use case, the provider organization offers patients a web-based application that enables the patient to query for, retrieve, view, use, and locally persist discrete clinical data elements or clinical summary documents. The use case provides the application programmatic access to all of the discrete data elements included in the Common MU Data Set. For example, an application might enable a patient to view a single lab result, or to request and retrieve a Clinical Summary document, or to identify relevant clinical trials from a national database. The data request may be a selectable function within the application (e.g., show me my visit summary), or the application may need to request data as input to a user-selectable function (e.g., chart my blood glucose levels over the past 3 months). Once the requested data or documents are retrieved, the application can work with them (e.g. by displaying to the patient, or using as the input to another function, or persisting for future use).

Actors

- Provider – organization that holds EHR data, provides a patient portal account, and approves web-based applications capable of accessing those data
- Patient – uses her browser to run the application that accesses her healthcare records to perform some useful task (e.g. visualization, interpretation, communication)
- Application – requests, and (on approval) accesses EHR data on the patient's behalf
- Authorization server – server used by EHR system to authenticate the clinician and to authorize the application to access EHR data on behalf of the clinician, in accordance with legal and institutional policies
- Resource server – server used by EHR system to hold and retrieve EHR data as authorized

Pre-conditions (outside scope of this use case)

- The provider has developed, selected, or otherwise approved a web-based software application that uses structured EHR data to help patients perform some valuable function (e.g. data visualization, interpretation, or communication).

- The provider has registered the application with the authorization server and has issued to the application credentials to enable it to authenticate its own identity.
- Provider organization operates in compliance with HIPAA Privacy and Security Rules.
- The application functions in accordance with the provider organization's privacy and security policy (e.g., runs on a trusted server, enables data persistence only in accordance with policy).
- The provider has identity-proofed the patient and has issued credentials (e.g., userID, password) for use in authenticating that identity.
- Provider holds the patient's health data.

Post-conditions

- The patient has run the application on her own EHR record, or else the patient has been given a reason why the request has not been fulfilled.
- The provider systems have recorded the access (audit is outside the scope of this use case).

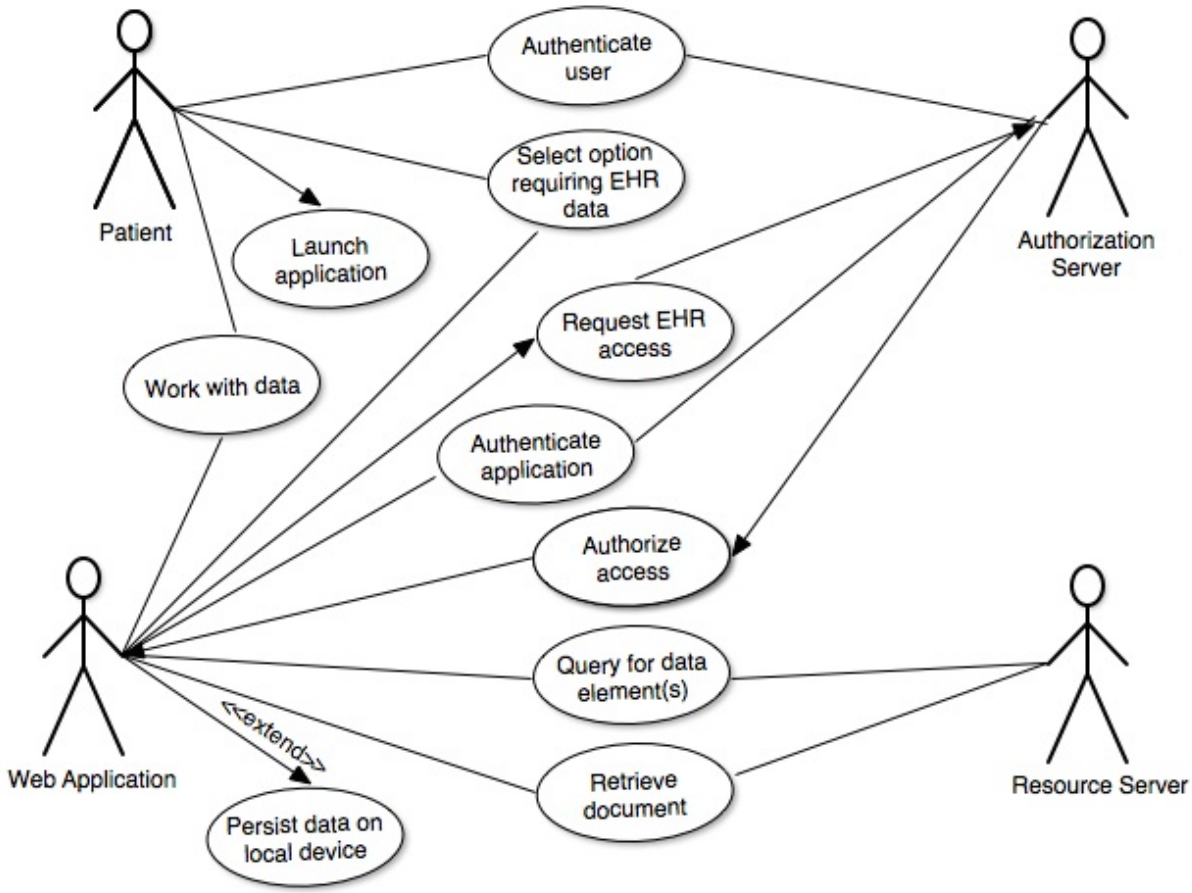
Basic Flow

1. Patient opens web browser and launches the application. (The workflow from which the application is launched is outside the scope of this use case.)
2. Patient selects an application option that requires that data be retrieved from the patient's EHR.
3. Application requests access to the desired data.
4. Authorization server authenticates the application's identity.
5. Authorization server authenticates the patient's identity.
6. Authorization server authorizes the application to retrieve the requested data within a limited period of time.
7. Application queries Resource Server for data elements
8. Resource Server returns the requested and authorized data elements, or indicates that the requested data are unavailable.
9. Application works with the retrieved data as requested by the patient, potentially persisting it for future use.
10. This use case ends when the patient logs out of the application, or the application server otherwise terminates the patient's session.

Alternative Flow

This flow is identical to the Basic Flow except that the application sends a request for a Clinical Summary document instead of querying for and retrieving discrete data elements.

UML Diagram for Use Case 1



Use Case 2: Patient uses provider-approved mobile app to access health data

Introduction

In this use case, the provider organization offers patients a mobile app that enables the patient to query for, retrieve, view, use, and persist discrete clinical data elements or clinical summary documents. The use case provides the app programmatic access to all of the discrete data elements included in the Common MU Data Set. For example, the app might help a patient view the result of a recent lab test, or to request and retrieve a Clinical Summary document, or to identify relevant clinical trials from a national database. The data request may itself be a selectable function within the app (e.g., show me my lab result from last week), or the app may request data as input to a user-selectable function (e.g.,

chart my blood glucose levels over the past 3 months). Once the requested data are retrieved, the patient is able to view the data or document, use the data as input to another function, or persist the data for future use, such as charting and presenting longitudinal data. Depending upon the app's architecture, as approved by the provider organization, the data may be persisted only on the mobile device or within the app's cloud-based server.

Actors

- Provider – organization that holds the EHR data and offers patients a mobile app for accessing those data
- Patient – downloads and installs the mobile app and uses it to access her data and perform some useful functions (e.g. visualization, interpretation communication)
- Mobile app – requests, and (on approval) accesses EHR data on the patient's behalf.
- App server (optional) – cloud-based server the app uses to persist data
- Authorization server – server used by EHR system to authenticate the clinician and to authorize the application to access EHR data on behalf of the clinician, in accordance with legal and institutional policies
- Resource server – server used by EHR system to hold and retrieve EHR data as authorized

Pre-conditions (outside scope of this use case)

- The provider has developed or selected a mobile app that uses structured EHR data to help patients perform some valuable function (e.g. data visualization, interpretation, or communication).
- The approved app may or may not be associated with a cloud-based server, but if the app enables storing data in a cloud environment, the cloud server is included in the approved software.
- The provider has registered the app with the authorization server.
- Provider organization operates in compliance with HIPAA Privacy and Security Rules.
- The app operates in accordance with the provider's privacy and security policy (e.g., enables data persistence only in accordance with policy).
- The provider has identity-proofed the patient and has issued credentials (e.g., userID, password) for use in authenticating that identity.
- Provider holds the patient's health data.

Post-conditions

- The patient has run the app to access her own record, or else the patient has been given a reason why the request has not been fulfilled.
- The provider systems have recorded the access (audit is outside the scope of this use case).

Basic Flow

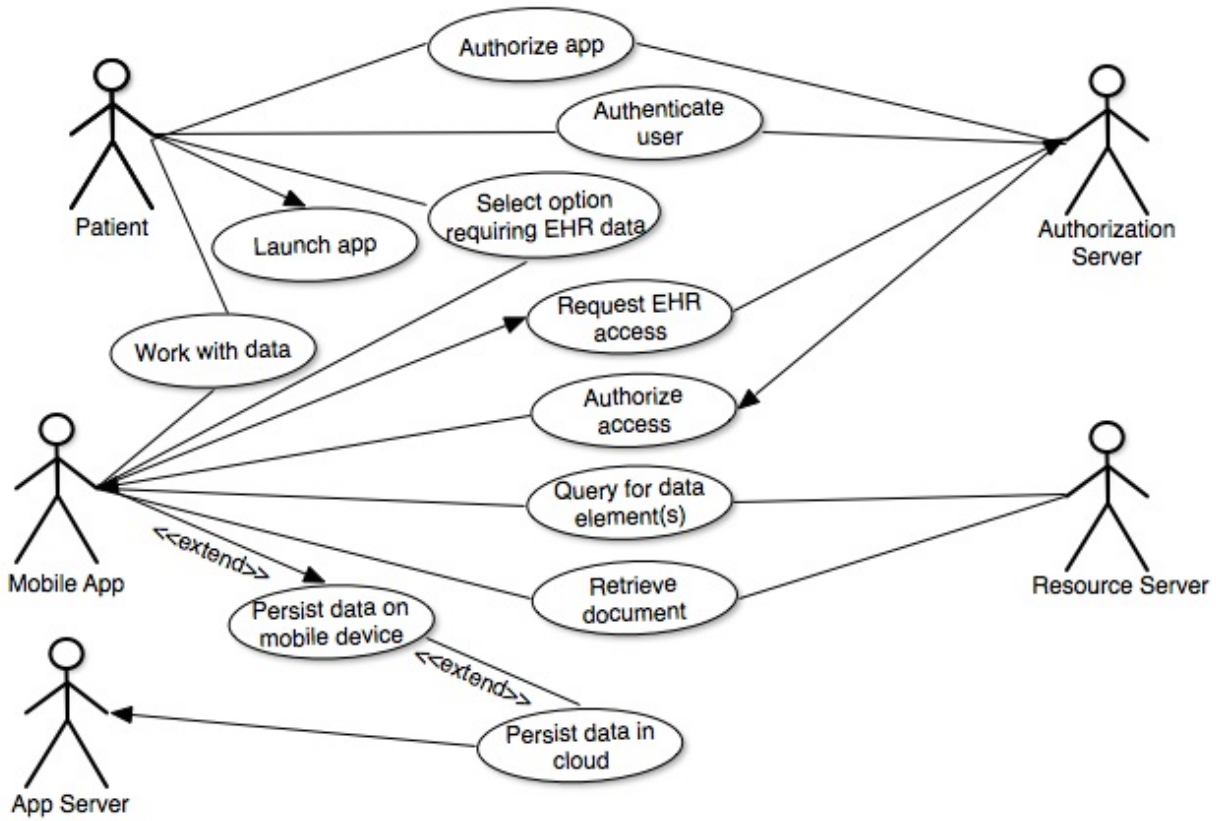
1. Patient opens the app. (The workflow from which the application is launched is outside the scope of this use case.)
2. Patient selects an app option that requires that data be retrieved from the patient's record held by the EHR system's resource server .
3. App requests access to the desired data.

4. Authorization server authenticates the patient's identity.
5. Authorization server asks patient to authorize the app to access the data.
6. Patient authorizes the app.
7. Authorization server authorizes the app to retrieve the requested data within a limited period of time.
8. App queries resource server for discrete data elements.
9. Resource server returns requested and authorized data elements, or indicates that the requested data are unavailable.
10. App uses the retrieved data as needed, potentially persisting it for future use to the mobile device or to a cloud-based server.
11. App may persist data for future use.
12. This use case ends when the patient no longer is using the app, or when the mobile device is shut down.

Alternative Flow

This flow is identical to the Basic Flow except that the app sends a request for a Clinical Summary document instead of querying for and retrieving discrete data elements.

UML Diagram for Use Case 2



Use Case 3: Clinician uses provider-approved web application to access health data

Introduction

In this use case, the provider organization offers its clinicians a web-based application that enables the clinician to query for, retrieve, view, use, and locally persist discrete data elements and clinical summary documents. The use case provides the application programmatic access to all of the discrete data elements included in the Common MU Data Set. For example, an application might enable a clinician to view a single lab result for a named patient, or to request and retrieve a Transition of Care or Clinical Summary document for a named patient. The data request may be a selectable function within the application (e.g., show me John Doe's Clinical Summary), or the application may need to request data as input to a user-selectable function (e.g., chart glucose blood levels for John Doe over the past 3 months). Once the requested data or documents are retrieved, the application can work with them (e.g., by displaying to the clinician, or using as the input to another function, or persisting for future use).

Actors

- Provider – organization that holds the EHR data, provides an EHR account, and approves web-based applications capable of accessing patients' data
- Clinician – uses her browser to run the application that accesses patient data to perform some useful task (e.g., visualization, interpretation, communication)
- Application – requests, and (on approval) accesses EHR data on the clinician's behalf
- Authorization server – server used by EHR system to authenticate the clinician and to authorize the application to access EHR data on behalf of the clinician, in accordance with legal and institutional policies
- Resource server – server used by EHR system to hold and retrieve EHR data as authorized

Pre-conditions (outside the scope of this use case)

- The provider has developed, selected, or otherwise approved a web-based software application that uses structured EHR data to help clinicians perform some valuable function (e.g. data visualization, interpretation, or communication).
- The provider has registered the application with the authorization server and has issued to the application credentials to enable it to authenticate its own identity.
- Provider organization operates in compliance with HIPAA Privacy and Security Rules.
- The application functions in accordance with the provider organization's privacy and security policy (e.g., runs on a trusted server, enables data persistence only in accordance with policy).
- The provider has identity-proofed the clinician and has issued credentials (e.g., userID, password) for use in authenticating that identity and clinician role.
- Provider holds the named patient's EHR data.

Post-conditions

- The clinician has run the application and accessed patient data, or else the clinician has been given a reason why the request has not been fulfilled.
- The provider systems have recorded the access (audit is outside the scope of this use case).

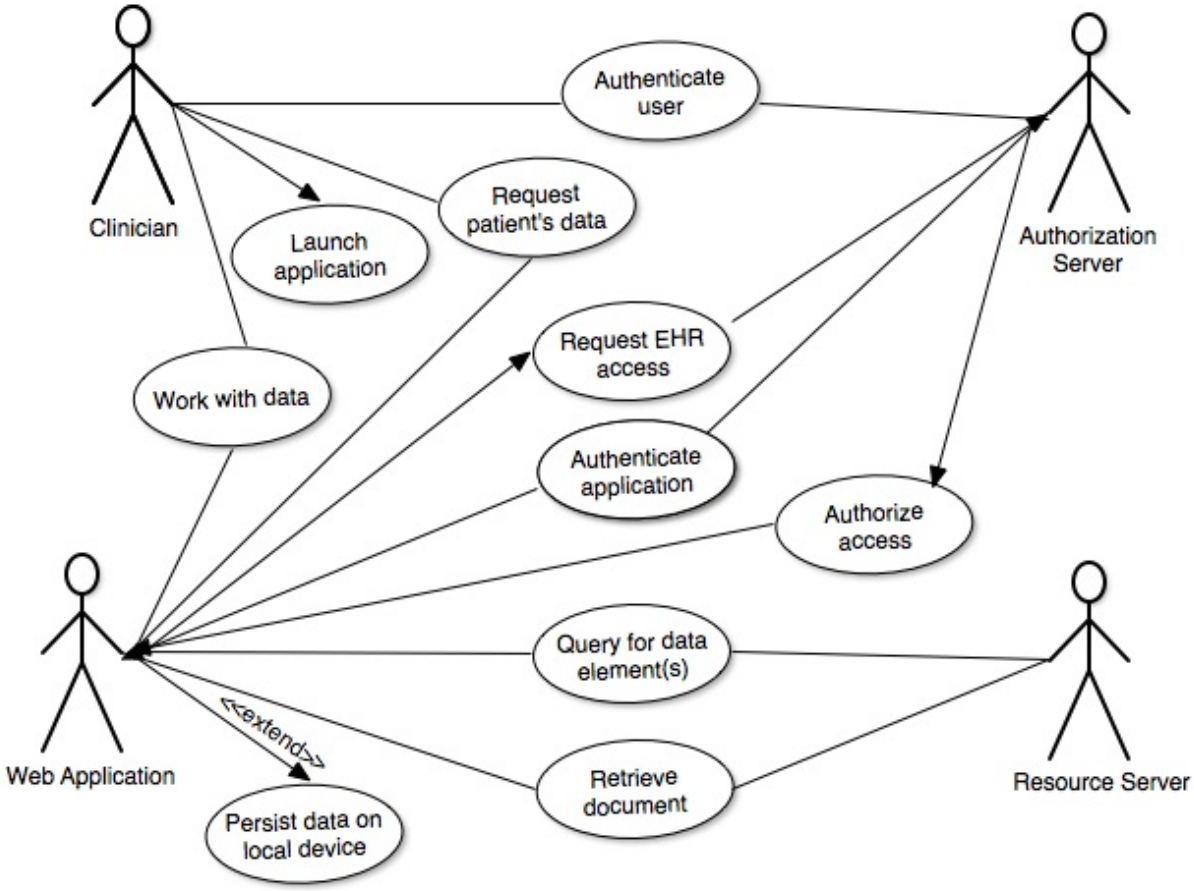
Basic Flow

1. Clinician opens web browser and launches the application. (The workflow from which the appl is launched is outside the scope of this use case.)
2. Clinician selects an application option that requires that data be retrieved from a named patient's EHR.
3. Application requests access to the desired data.
4. Authorization server authenticates the application's identity.
5. Authorization server authenticates the clinician's identity and role.
6. Authorization server authorizes the application to retrieve the requested data within a limited period of time.
7. Application queries EHR system for data elements
8. Resource server returns the requested and authorized data elements, or indicates that the requested data are unavailable.
9. Application works with retrieved data in web browser.
10. Application may persist data for future use.
11. This use case ends when the clinician logs out of the application, or the application server otherwise terminates the clinician's session.

Alternative Flow

This flow is identical to the Basic Flow except that the application sends a request for a Transition of Care or Clinical Summary document instead of querying for and retrieving discrete data elements.

UML Diagram for Use Case 3



Use Case 4: Clinician uses provider-approved mobile app to access health data

Introduction

In this use case, the provider organization offers clinicians a mobile app that enables the clinician to query for, retrieve, view, use, and persist discrete data elements or a document containing a summary of a named patient's EHR data. The use case provides the app programmatic access to all of the discrete data elements included in the Common MU Data set. For example, the app might help a clinician view the result of a patient's recent lab test, or to request and retrieve a Clinical Summary or Transition of Care document. The data request may itself be a selectable function within the application (e.g., show me John Doe's Clinical Summary), or the application may need to request data as input to a user-selectable function (e.g., chart glucose blood levels for John Doe over the past 3 months). Once the requested data are retrieved, the clinician is able to view the data or document, use the

data as input to another function, or persist the data for future use, such as charting and presenting longitudinal data. Depending upon the app's architecture, as approved by the provider organization, the data may be persisted only on the mobile device or within the app's cloud-based server.

Actors

- Provider – organization that holds the EHR data and offers clinicians a mobile app for accessing patients' EHR data
- Clinician – uses a mobile app to select options for retrieving, viewing, manipulating, and saving data
- Mobile app – queries for and retrieves data, as requested and authorized
- App server – cloud-based server the app uses to persist data
- Authorization server – server used by EHR system to authenticate the clinician and to authorize the application to access EHR data on behalf of the clinician, in accordance with legal and institutional policies
- Resource server – server used by EHR system to hold and retrieve EHR data as authorized

Pre-conditions (outside the scope of this use case)

- The provider has developed or selected a mobile app that enables clinicians to query for, retrieve, view, and persist data elements and summary documents for named patients.
- The approved app may or may not be associated with a cloud-based server, but if the app enables storing data in a cloud environment, the cloud server is included in the approved software.
- The provider has registered the app with the authorization server and has issued to the app credentials to enable it to authenticate its own identity.
- Provider organization operates in compliance with HIPAA Privacy and Security Rules.
- The app operates in accordance with the provider's privacy and security policy (e.g., enables data persistence only in accordance with policy).
- The provider has identity-proofed the clinician and has issued credentials (e.g., userID, password) for use in authenticating that identity and clinician role.
- Provider holds the named patient's EHR data.

Post-conditions

- The clinician has found, viewed, and possibly downloaded the requested data; else the clinician has been given a reason why the request has not been fulfilled.
- The provider system has recorded the access (audit is outside the scope of this use case).

Basic Flow

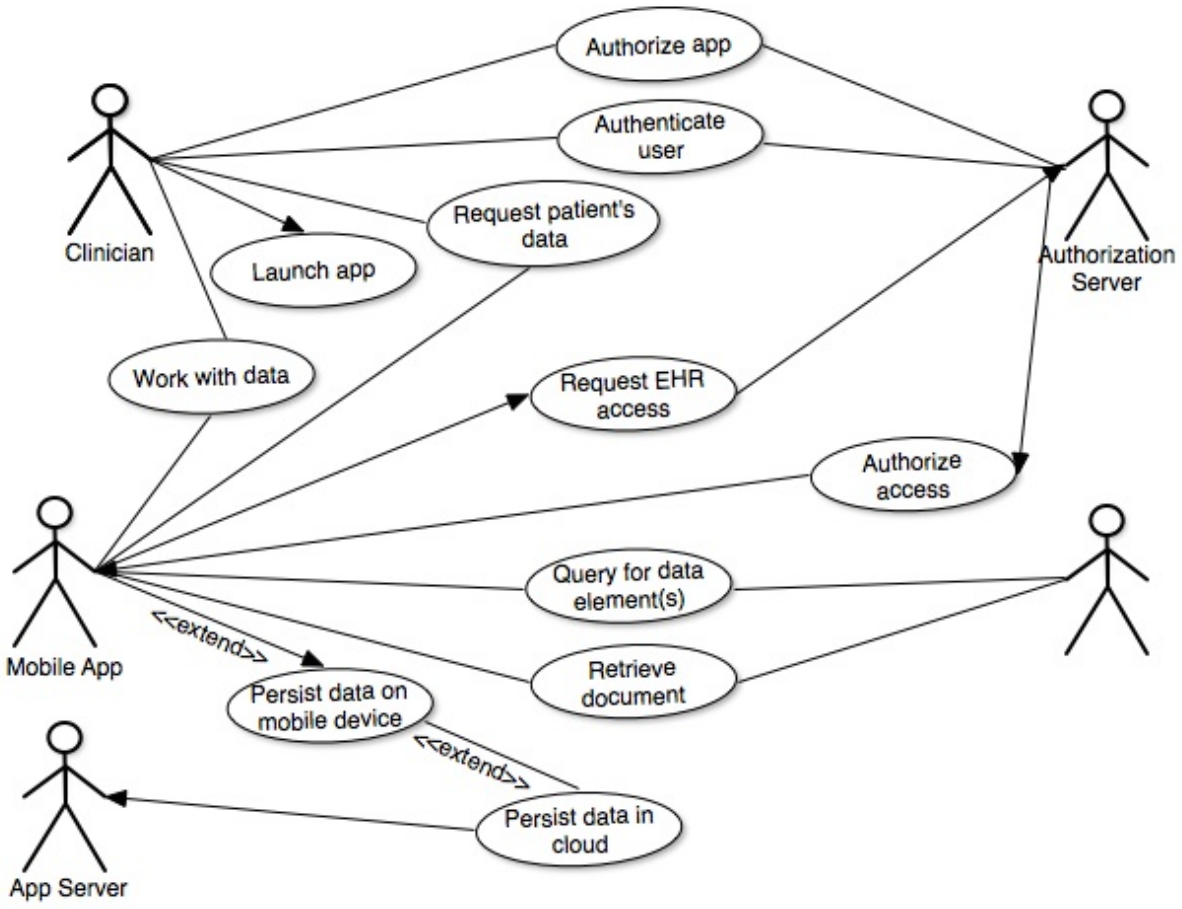
1. Clinician opens the app. (The workflow from which the app is launched is outside the scope of this use case.)
2. Clinician selects an app option that requires that data be retrieved from a named patient's EHR.
3. App requests access to the desired data.

4. Authorization server authenticates the clinician's identity and role.
5. Authorization server asks clinician to authorize the app to access the data.
6. Clinician authorizes the app.
7. Authorization server authorizes the app to retrieve the requested data within a limited period of time.
8. App queries resource server for discrete data elements
9. Resource server returns the requested and authorized data elements, or indicates that the requested data are unavailable.
10. App works with retrieved data.
11. App may persist data for future use.
12. This use case ends when the clinician no longer is using the app, or when the mobile device is shut down.

Alternative Flow

This flow is identical to the Basic Flow except that the app sends a request for a Transition of Care or Clinical Summary document instead of querying for and retrieving discrete data elements.

UML Diagram for Use Case 4



Use Case 5 (future: Provider using EHR A access patient record held in EHR B

Introduction

In this use case, the clinician uses an EHR application (EHR A) that allows the clinician to query for, retrieve, view, use, and locally persist discrete clinical data elements or clinical summary documents held in EHR B. The use case provides the application programmatic access to all of the discrete data elements included in the Common MU Data Set. For example, an application in EHR A might enable the clinician to view a single lab result, or to request and retrieve a Clinical Summary document, or to graph blood pressure results over time using data from EHR B. Once the requested data or documents are retrieved, EHR A can work with them (e.g. by displaying to the clinician, or using as the input to another function, or persisting for future use).

Actors

- Clinician – authorized clinical user of EHR A
- Provider A - the organization to which clinician belongs
- EHR A – clinical application provided by Provider A for Clinician's use in accessing resources held by Provider A and trusted partners
- EHR B resource server - clinical application that holds and manages patient records held by Provider B
- Provider B - the organization that has authority over EHR B
- Provider B designated authorization server – authorizes access to resources held by Provider B on behalf of the Clinician, in accordance with legal and institutional policies

Pre-conditions (outside scope of this use case)

- The Clinician has authenticated herself to EHR A, which is capable of fulfilling the functions described in this document.
- EHR B is capable of fulfilling the functions described in this document
- Provider B has agreed to trust Provider A's applications and clinicians to access Provider B's clinical records for certain uses.
- Provider A has proof of organizational identity that is trusted by Provider B
- Provider B trusts Provider A to perform essential security and authentication functions (e.g., to authenticate Clinician) and trusts the data use request claims made by Provider A.
- EHR B resource server holds the patient's health data.
- EHR A and EHR B can link patient identity to the patient.
- Providers A and B operate in compliance with HIPAA Privacy and Security Rules.
- Patient is a competent adult and patient data contains no sensitive information requiring special protections (e.g., SAMHSA protected Part 2 data, HIV status, etc.)

Post-conditions

- The Clinician using EHR A has accessed the patient record in EHR B, or else the Clinician has been given a reason why the request has not been fulfilled.
- EHR A and EHR B have recorded the access (audit is outside the scope of this use case).

Basic Flow

1. Clinician uses EHR A. (The workflow from which the EHR A is launched is outside the scope of this use case.)
2. Clinician selects an EHR option that requires that data be retrieved from EHR B.
3. EHR A requests access to the desired patient's data in EHR B for HIPAA-defined treatment purposes.
4. EHR B authorization server authenticates itself to EHR A and establishes a secure link.
5. EHR B authorization server accepts the proof of organizational identity proffered by EHR A and accepts the ID token containing claims regarding the authenticated Clinician.
6. EHR B authorization server authorizes EHR A to retrieve the requested data, on behalf of the Clinician, within a limited period of time.
7. EHR A queries EHR B resource server for data elements..
8. EHR B resource server returns the requested and authorized resources,, or indicates that the requested data are unavailable.
9. EHR A works with the retrieved data as requested by the Clinician, potentially persisting it for future use.
10. This use case ends when the Clinician completes the use of EHR A functions working with the requested patient's data.

Alternative Flow

This flow is identical to the Basic Flow except that EHR A sends a request for a Clinical Summary document instead of querying for and retrieving discrete data elements.

UML Diagram for Use Case 5