Project HealthDesign
Common Platform Components
Functional Requirements

Version 1.0

December 7, 2007

Prepared by

Sujansky & Associates, LLC

Support for this work was provided by a grant from

The California HealthCare Foundation

in Partnership with

The Pioneer Portfolio of the Robert Wood Johnson Foundation

Revision History

Version	Author/Editor	Date	Comment
0.1	Walter Sujansky / Sam Faus Sujansky & Associates, LLC www.sujansky.com	10/30/2007	Draft
0.9	Walter Sujansky	11/23/2007	Pre-baselined version, pending final review
1.0	Walter Sujansky	12/07/2007	Baselined version

Table of Contents

Tables

Figures

1. Introduction

Personal health applications (PHAs) are software tools that assist consumers to track and manage the health status and medical conditions of themselves and their families. Project HealthDesign is a research initiative sponsored by the Robert Wood Johnson Foundation and the California HealthCare Foundation to explore the design of advanced PHAs that address various health conditions and wellness goals. Among the objectives of Project HealthDesign is the identification and characterization of software components that provide functionalities common to many PHAs. These components are part of an envisioned infrastructure, or *common platform*, that can accelerate the development of new PHAs and facilitate interoperability among them.

This document describes the requirements of *Common Platform Components* (CPCs) in four target areas:

1. *Medication List Management*: Resources to help PHAs record, manage, share, and provide advice based on the list of specific medications that a patient takes regularly.
2. *Calendaring*: Resources to help PHAs record, track, share, and remind patients of specific scheduled events that are relevant to the management of their health or medical conditions.
3. *Observations captured in the course of daily living*: Resources to help PHAs store, aggregate, analyze, and share data recorded by patients that are relevant to the management of their health or medical conditions and that are captured outside of their encounters with the health care system.
4. *Identity Management*: Resources to help PHAs manage the list of users and software systems that are authorized to access patient-specific data, authenticate the identity of users and systems that are requesting access to these data, and allow patients to monitor and precisely control the access that is provided to their health data.

Project HealthDesign identified these areas as specifically relevant to the nine PHA projects currently underway, and the requirements-development process sought to identify the specific functional needs of the projects (see www.ProjectHealthDesign.org/projects for descriptions of the nine projects). In particular, the requirements address the following aspects of the projects' needs in the target areas:

- The tasks that PHAs typically perform that involve the target areas
- The ways that data related to the target areas are typically entered or captured by PHAs
- The ways that stored data related to the target areas are typically retrieved, processed, or exported by PHAs
- The data in the target areas that PHAs need to store and access in a structured and/or coded form to enable automated processing (such as reporting, aggregation, or analysis)
- The capabilities and functions that PHAs require from software components in each of the target areas to meet their operational needs

2. Common Platform Components: Purpose and Use

Before reviewing the specific requirements that were collected, it is useful to consider the "big picture" with respect to common platform components for personal health applications. First, the development of common platform components has two primary purposes:

1. To *facilitate the development* of personal health applications by making available commonly needed software resources that would otherwise have to be designed and built from scratch by each PHA project.

2. To *promote interoperability* among personal health applications by defining standard data models and interchange formats for personal health data and by providing shared data repositories and software services that multiple PHAs may access.

Although related, these purposes are not identical, as described below.

2.1. Facilitating Development of PHAs

CPCs may comprise modular software resources that provide functionality commonly needed by and similar in function across various PHAs. For example, many PHAs require a calendaring function to help patients manage their schedules for medication dosing, physiological measurements, physician appointments, exercise, and other health-related events. Also, PHAs frequently require a formal data model and coding system for prescription medications so that they may provide advice automatically about appropriate dosing, drug interactions, and cost-effective drug purchasing. If a calendaring module or a structured medication terminology that meets the PHA's needs is already available, the developers of PHAs can *incorporate* these resources into their applications. Although the incorporation of CPCs directly into PHAs will not necessarily confer interoperability among them, it will obviate the need for the developers to design and develop the components from scratch.

There are at least three types of CPCs that can facilitate PHA development:

1. Functioning software components that may be tightly integrated into PHAs (such as source code modules or compiled libraries) or remotely accessed by PHAs (such as network-resident services). As a general example of such a component, database management systems, such as Oracle or SQLServer, are essentially network resident CPCs that most applications use, obviating the need to develop a robust and high-performance data-management system from scratch.
2. Conceptual models that define clinical data elements, database schemas, functional requirements, and/or API specifications for PHAs. These CPCs facilitate development by providing proven and comprehensive models that avoid much redundant requirements analysis and design work. For example, the functional requirements, data model, and API specifications of a module that manages user authentication and access control is a valuable resource for the developers of PHAs, even if they must still implement the specifications of the module.
3. Medical content that PHAs display to users or require for decision-support functionality. For example, hierarchically structured terminologies for medical concepts (such as drugs, diseases, symptoms, etc.); mappings between coding systems (such as NDC-to-RxNorm mappings, or ICD-9 to SNOMED mappings); rule bases for decision support (such as drug-drug interaction checking); and reference content (such as images of pills and drug monographs for use by patients). Although these resources already exist in many cases, they are often costly or difficult to find. Public domain, open-source, or royalty-free versions of such resources could facilitate the development of PHAs

2.2. Promoting Interoperability Among PHAs

CPCs can also provide a shared infrastructure to promote interoperability among PHAs. Interoperability is valuable because it allows patient data to be collected only once and thereafter shared by different PHAs for different purposes. For example, a shared data repository of observations on drug administration times, blood glucose measurements, symptom reporting, meal composition, and physical activity could be used by one PHA to counsel an elderly diabetic patient on optimum insulin dosing and another PHA to counsel the same patient on management of heart failure. Also, the use by two PHAs of a common data model and coding system for medications (even in the absence of a shared data repository) could facilitate the exchange of medication data between the PHAs by minimizing the syntactic and semantic heterogeneity of these data.

There are two types of CPCs that promote interoperability:

1. Shared data repositories and data models. These CPCs provide a common data platform and common data model that enable one PHA to access and correctly process data that was collected via another PHA. An example of such a resource is a single medication list shared by two PHAs, one that collects prescription medications from a patient and counsels the patient on appropriate dosing regimens, and the other that automatically notifies the patient when less costly sources of the prescribed medications are available. It's important to note that a shared data store, unto itself, does not provide interoperability in the absence of a shared data model (i.e., a common structure and coding of data), because data stored by a PHA that uses one data model may not be useful to another PHA using a different model.
2. Messaging and terminology standards. The collective implementation of an appropriate messaging or terminology standard among multiple PHAs can provide a common platform for sharing data, even in the absence of any common software modules or shared data repositories. For example, if a set of PHAs agree to exchange medication data using the NCPDP Script v8.1 data structure and the RxNorm Clinical Drug codes, then semantic interoperability may be achieved even if each PHA stores its own copy of medication data per its own internal data model and coding system. As long as the translations between the internal representation formats and the standard data-exchange format are faithful, the PHAs will be able to exchange medication data correctly.

2.3. Use of Common Platform Components

Common platform components may be used in various ways to facilitate the development of PHAs and/or promote interoperability among them. Figure 2.1 - Figure 2.3 illustrates several of these configurations. In Figure 2.1, several CPCs ("C1" – "C3") are tightly integrated into two standalone PHAs. The PHAs have need for the functionality provided by these CPCs and integrate them with the other modules that already exist. This reuse of available CPCs is convenient from a software-development perspective, but does not promote interoperability.

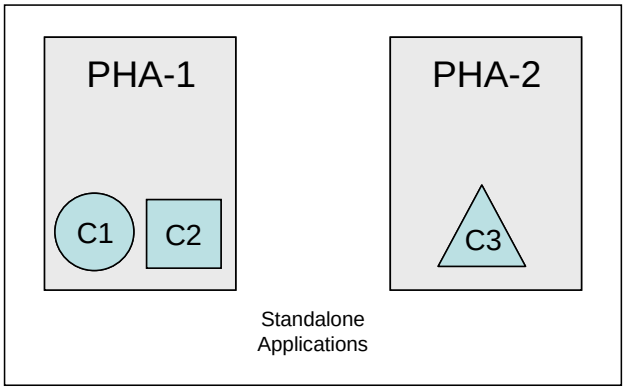

Figure 2.1 Use of common platform components in stand-alone PHAs.

In Figure 2.2, several CPCs are again tightly integrated into two PHAs, but because one of the predefined components and its application programming interface ("C2") is common to the two applications, data relevant to that component may be more easily exchanged between them. For example, if two PHAs use the same medication-list component, the common structure and coding of medications will make it much easier for the two to exchange medication list records.

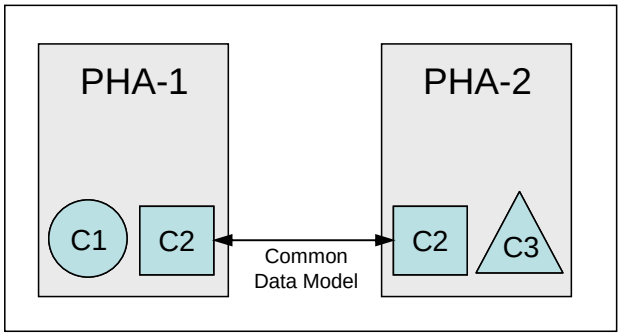

Figure 2.2 Use of "tightly integrated" common platform components to promote interoperability

In Figure 2.3, two components are again tightly integrated into the PHAs, but a third component ("C2") is "loosely coupled" with the PHAs, enabling them to share the component as a common data repository. This configuration ensures that both applications are using the same version of the patient's data and that no variance in the syntactic or semantic representation of the data exists between them.

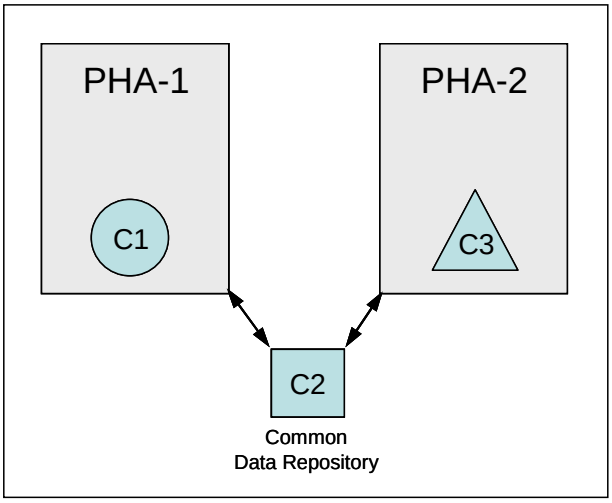

Figure 2.3 Use of a "loosely coupled" common platform component to promote interoperability

Because the need for and willingness of distinct PHAs to share common data repositories and software services has not been established in practice, we have not presumed whether common resources will be implemented as single shared instances that are "loosely coupled" with multiple PHAs or as multiple distinct instances that are each "tightly integrated" into a single PHA. The requirements documented here attempt to accommodate either strategy for using the common platform components.

3. Notation

Most of the requirements are listed in tables with two columns:

Req ID: A unique identifier for the requirement, for reference purposes

Requirement: A description of the requirement, with examples where relevant

4. Medication List Management

The Medication List Management component (CP:MED) is intended to store and make available to PHAs the set of medications that patients take regularly.

4.1. PHAs and Medication Lists

A first step in defining the functional requirements of a medication-list component is to enumerate the functions that PHAs may need to perform related to medication lists. Table 4.1 lists these requirements, as elicited from the nine grantees of Project HealthDesign.

Table 4.1. PHA functions that require medication list management

No.	Function
1	Display to patients the list of medications that they take regularly, including prescription medications, over-the-counter medications, and "alternative" medications (supplements, herbals, etc.)
2	Display to patients the dosing instructions for each of the medications on their medication list
3	Display to patients relevant reference information about each of the medications on their medication list (such as possible side effects, images of the pills or capsules that they were dispensed, reason for taking the medication, etc.)
4	Display the contents of a patient's current medication list to others who are involved in the patient's care, such as family members, care givers, and health care providers. This sharing may be achieved by a patient granting access to her electronic medication list to selected users or by simply printing out a copy of the list to show to others.
5	Export a patient's medication list in an electronic format that can be imported by other health record applications
6	Help patient to develop specific schedules for the administration of certain medications on their medication lists so that the schedules are consistent with both the prescribed dosing of the medications and the patients' personal schedules and preferences
7	Check for harmful interactions among the medications on a patient's medication list
8	Check for unintended duplication of therapy among the medications on a patient's medication list
9	Help patients to identify less costly options for procuring the medications on their medication lists (such as lower-cost sources for the same medications or generic equivalents of brand-name medications)
10	Help patients to remember to stop certain of their medications prior to surgical procedures (such as anti-coagulants)
11	Help family members, caregivers, or health care professionals assess a patient's compliance with the prescribed dosing for each medication on the patient's medication list by tracking how frequently the patient receives refills relative to the expected rate at which the patient's supply of the medication should be consumed.
12	Help patients to tailor the selection and dosing of medications to their pharmocogenomic profiles.

4.2. Sources of Data for Medication Lists in Personal Health Records

The CP:MED component must support a variety of data-acquisition methods, because medication lists for personal health records may be generated in a variety of ways. The set of data-acquisition methods that the component must support, in turn, influences the data elements, coding systems, and degree of flexibility in data capture that the component shall need to support.

Table 4.2. Requirements for Medication List Common Platform Component: Data Sources

Req ID	Requirement
MED- 1	The component shall have the ability to store prescriptions that are electronically imported from external EHR data repositories, which may contain variable degrees of structure and coding [E.g., from an EHR that can export medication records via HL7 messages or CCR documents]
MED- 2	The component shall have the ability to store prescription data that are manually entered by the prescribing physician in a manner that is controlled by a PHA [i.e., the PHA can control the degree of structure and coding of the data]
MED- 3	The component shall have the ability to store prescription data that are manually entered by the patient or another lay person in a manner that is controlled by a PHA and that is based on information appearing on the prescription that the patient received from a physician.
MED- 4	The component shall have the ability to store dispense records that are electronically imported from external systems that may contain variable degrees of structure and coding, but at a minimum include the NDC codes for dispensed medications [E.g., a pharmacy, pharmacy benefit manager, or payer via batch files or real-time EDI transactions]
MED- 5	The component shall have the ability to store dispense records that are manually entered in a manner that is controlled by a PHA and based on information appearing on the label of the dispensed medication.
MED- 6	The component shall have the ability to store dispense records for prescription, over-the-counter, and alternative medications that are manually entered via a PHA based on whatever information a patient may have about her medications (possibly just the name)

4.3. Data Model for the Medication-List Component

To support the storage, processing, and interoperability needs of PHAs with respect to medication lists, the component must provide a structured, consistent, and sufficiently rich data model. Although the component need not necessarily implement that data model internally, its interface to PHAs and other external systems must support the syntax and semantics of the data model. This consistency will provide a well-defined interface between the component and PHAs, and it may allow multiple PHAs to effectively share a single patient medication list.

Note that the data model is intentionally general and flexible to accommodate medication list records that are entered via any of the methods listed in Table 4.2. For example, a medication may be identified by its NDC code if it is imported as a dispense record from a pharmacy, by its RxNorm clinical drug code if it is imported from an EHR med list, or by its name alone if it is manually entered by a patient.

4.3.1. Types of Medication List Records

There are several types of records that may be captured and stored in the CP:MED component, the characteristics of which vary based on the source of the medication data and the method by which they were collected.

Table 4.3. Types of Medication List Records

Req ID	Requirement
MED- 7	The component shall have the ability to store a medication *prescription*, i.e., the identity of a medication, the amount to be dispensed, the dosing instructions, and any refill allowances as specified by the prescribing physician.
MED- 8	The component shall have the ability to store a medication *dispense record*, i.e., the identity and quantity of the actual medication product dispensed by a pharmacy, physician, or over-the-counter outlet, as well as the dosing instructions provided with the dispensed medication, and any refill allowances granted by the dispenser. Note that certain of these data may be different from those in the corresponding medication prescription (e.g., a generic equivalent may be dispensed, although a brand-name drug was prescribed).
MED- 9	The component shall have the ability to store an *ad hoc* medication record, i.e. information regarding a medication taken by a patient that is derived from neither a prescription nor a specific dispense record. For example, a patient may be taking an over-the-counter medication, such as baby aspirin or chondroitin sulfate, that is purchased regularly and repeatedly by the patient. It would not be useful to enter each purchase ("dispense record") of such a medication, nor is there a prescription for it.

4.3.2. Attributes of Medication List Records

Based on the intended functions, sources of data, and types of records that the medication-list management component is required to support, medication list records shall consist of the data attributes listed in Table 4.4.

Table 4.4. Attributes of Medication List Records

Req ID	Requirement
	For each medication record in the medication list, the component shall be able to store the following data elements
MED- 10	• Medication Record Unique ID (text) [Note: Assigned automatically by the component. The component shall assign a unique ID to each distinct medication record, with "distinct medication record" defined as a specific prescription for a medication, dispensing of a medication, or ad hoc recording of a medication. For example, if a medication record is *updated* to reflect a change in the prescribed frequency, that will not require the creation of a new record. If the identity of the medication is changed (e.g., from a brand to a generic), that will require a new medication record.]]
MED- 11	• Patient Record ID (text) [Note: this attribute stores the unique identifier of the patient record to which this medication record applies.]

MED- 12	• Medication Record Type [E.g.., “prescription”, “dispense record”, or “ad hoc”]
MED-12.1	• Medication Record Sub-Type (format TBD) [Note: PHAs may arbitrarily assign sub-types to medication records to assist in the processing of these records. For example, a PHA may store additional structured data for a medication record (i.e., data not defined by the common platform data model – see the Additional Structured Data attribute below), and the Sub-Type designator allows PHAs to retrieve and process medication records specific to the sub-types that they have defined. The Sub-Type value must consist of a Sub-Type designator and the unique identifier of the PHA that created the observation record (to ensure uniqueness for the Sub-Type designators across PHAs)]
MED- 13	• Identity of the medication as prescribed, dispensed, or described by user (text, code, and coding system) [E.g., “Lotensin” | “875764993” | “NDC”]
MED- 14	• Identity of the generic ingredient(s) of the medication (text, code, and coding system) [E.g., “benazepril” | “74885933” | “RxNorm/IN”]
MED- 15	• Medication unit strength (text, strength value, coded strength units, units coding system) [E.g., “10 mg” | “10” | “578932” | “Snomed” {code = “milligrams”}]
MED- 16	• Medication dosage form (text, code, and coding system) [E.g., “tablet” | “84732934” | “RxNorm/DF” {code = “tablet”}]
MED- 17	• Medication intended route (text, code, and coding system) [e.g., “by mouth” | “8293842” | “Snomed” {code = “oral”}]
MED- 18	• Medication intended or actual quantity dispensed and units (quantity dispensed, units text, units code, units Coding System) [E.g., “100” | “tablet” | “485738” | “RxNorm/DF” {code = “tablet”}]
MED- 19	• Medication intended dosing frequency (text, code, and coding system) [E.g., “once per day” | “8579347” | “PHD” {code = “bid”}]
MED- 20	• Medication intended dosing quantity and units (text, quantity value, coded quantity units, units coding system) [E.g., “2 tablets” | “2” | “485738” | “RxNorm/DF” {code = “tablet”}]
MED- 21	• Medication intended dosing conditions and other instructions (text only) [E.g., “for breakthrough pain”, “take with food”]
MED- 22	• Medication intended number of refills (integer)
MED- 23	• Complete description of the prescription and/or dispense data for the medication as a single text string (text only) [E.g., “Lotensin 10mg tabs, 2 tablets by mouth once per day, take with food; disp 100 tabs, no refills” [Note: to allow the import of entirely unstructured medication data from external systems]

MED- 24	• Out-of-pocket cost for the prescribed/dispensed quantity of the medication (formatted currency) [E.g., "$45.00"]
MED- 25	• Reference/link to Calendar events related to the medication [format TBD] [Note: this attribute allows the users of a PHA to navigate from a medication-list record to the specific schedule for taking the medication, if one has been specified]
MED- 26	• Reference/link to Observation records related to the medication [format TBD] [Note: This attribute allows the users of a PHA to navigate from a medication-list record to the patient-entered observations that document when the medication was actually taken, if such observations have been recorded.]
MED- 27	• Reference/link to other Medication-List records related to the same medication [format TBD] [Note: This attribute allows a PHA to navigate from a prescription to the corresponding dispense records or from one dispense record to a subsequent dispense record (i.e., when multiple refills have been dispensed)]
MED- 27.1	• Annotations (text) [E.g., "Remind Grammy to take this medication with food"] (Note: These annotations may be entered by other users, as permitted by the relevant access controls. Each annotation shall include a timestamp and the identity of the user who inserted it.)
MED- 27.2	• Additional Structured Data (structured text) [Note: This attribute shall store an ASCII-encoded text blob (structured or unstructured) that may be inserted and accessed by one or more PHAs. The structure and/or coding used within this field (such as XML) shall be defined *ad hoc* by the PHAs that use the field; i.e., it will not be part of the data model of the medication list component itself.
MED- 28	• Medication dosing status [Allowed values = "active", "on hold", "discontinued"] (whether the patient is currently taking the medication)
MED- 29	• Medication Record Effective Start Date [i.e., the date on which the prescription was written, the medication was dispensed to the patient, or the patient indicates that she began taking the medication]
MED- 30	• Medication Record Effective End Date [i.e., the date on which the medication dosing status of a medication record was changed to "discontinued"]

4.3.3. Terminology Requirements for Medication List Records

The data model requirements listed above imply certain requirements for controlled terminologies and coding systems. These specific requirements are listed below.

Table 4.5. Terminology Requirements for Medication List Records

Req ID	Requirement
MED- 31	*The component shall suggest one or more controlled terminologies that allow the identities of medications to be captured in a coded format at the following levels of abstraction.*
MED- 32	• Brand name only
MED- 33	• Generic name only
MED- 34	• Brand name + dosage form + dosage strength
MED- 35	• Generic name + dosage form + dosage strength
MED- 36	• NDC code
MED- 37	The controlled terminology for medications shall support mapping between the brand names of medications and the generic ingredients of those medications
MED- 38	The controlled terminology for medications shall support mapping between NDC codes and all other levels of abstraction for medication coding
MED- 39	The controlled terminology for medications shall support mapping between each of the levels of abstraction at which medications may be coded and a hierarchy of therapeutic classes
MED- 40	The component shall define a controlled terminology for the dosage forms of medications [e.g., “oral tablet”, “syrup”, “I.V. solution”, “transdermal patch”, etc.]
MED- 41	The component shall define a controlled terminology and/or representation syntax for prescribed frequencies of medication administration [e.g., “qd”, “bid”, “qAM”, “q4h”, etc.]
MED- 42	The component shall define a controlled terminology for the routes of administration of medications [E.g., “oral”, “intramuscular”, “transdermal”, “inhaled”, etc.]
MED- 43	The component shall define a controlled terminology for units of measure pertaining to dosage strengths [e.g., “mg,” “mg/ml”, etc.]

One general model for coding the identities of medications that is consistent with these requirements is proposed in Figure 4.1 below. This model is based on the structure of the RxNorm terminology that has been developed by the National Library of Medicine, but includes a few variations and extensions.

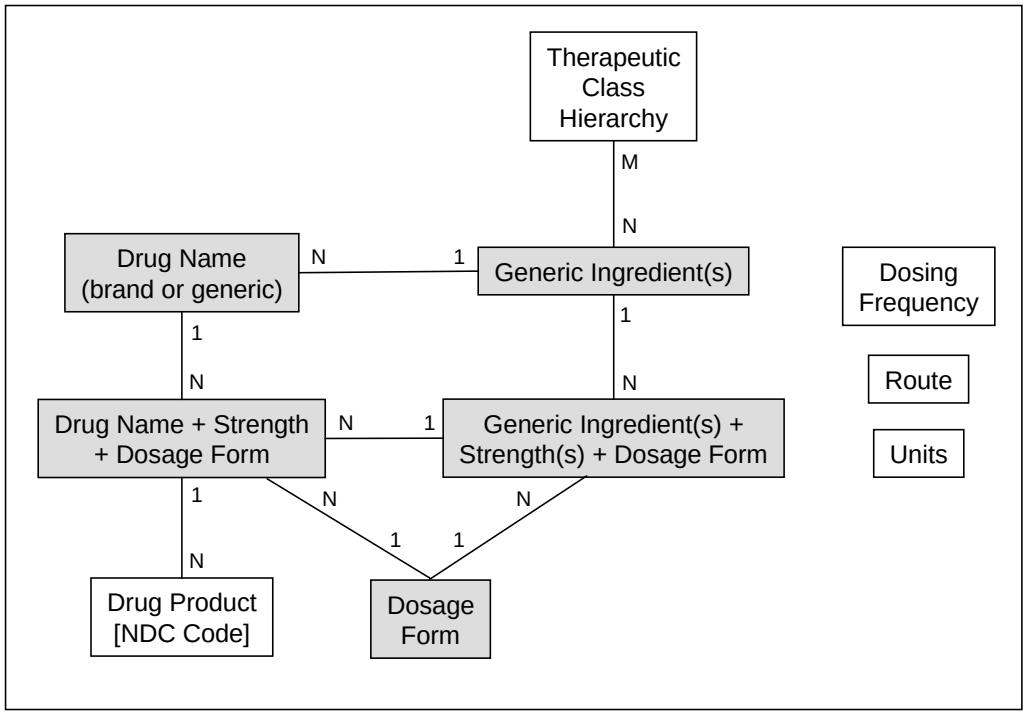

Figure 4.1 Proposed terminology model for medication lists.

In Figure 4.1, the shaded boxes and the lines that join them represent concepts and relationships that, for the most part, already exist in RxNorm (particularly, for single-ingredient drugs). The clear boxes and the lines emanating from them represent concepts that do not yet exist in RxNorm, but are required by PHAs for at least certain medication-list management functions.

4.4. Required Functionality for the Medication-List Management Component

Beyond data structures and terminologies, there also exist a set of requirements for the functions that a medication-list component must provide to PHAs. It is envisioned that these functions will be provided to PHAs via API calls.

Table 4.6. Required functionality for the medication-list management component

Req ID	Requirement
MED- 44	For any medication on a patient's medication list, the component shall have the ability to store the *prescription*, the *dispense record*, an *ad hoc* record, or any combination of the three. If multiple records are stored for the same medication, the component shall have the ability to explicitly represent the association between these records.
MED- 45	The component shall have the ability to insert a new medication record into the medication list for an existing patient when a PHA supplies all of the required attribute values, and the PHA represents all attribute values using allowed formats and coding systems.
MED- 46	The component shall have the ability to modify an existing medication record (identified by its Medication Record Unique ID) when a PHA represents all of the updated attribute values using allowed formats and coding systems.

MED- 47	The component shall have the ability to delete an existing medication record, as identified by its Medication Record Unique ID (for example, if a prescription or dispense record was entered erroneously).
MED- 48	The component shall make all modifications to and deletions of existing medication records "non-destructively," i.e., a record of the previous values of any modified or deleted medication records will be retained within the system, along with a record of when the modification/deletion occurred and which user requested it (see Audit Logging in Section 7.5).
MED- 49	The component shall have the ability to return to a PHA all attributes of all the medication records for a specified patient in a single operation
MED- 50	*The component shall have the ability to return to a PHA a subset of the medication records for a specified patient based on query expressions that include comparisons (>, <, =, LIKE) and Boolean combinations (AND, OR, NOT) involving the following attributes:*
MED- 51	• Medication Record Unique ID
MED- 52	• Identity of the medication as prescribed or dispensed (text and/or code)
MED- 53	• Generic identity of the medication (text and/or code)
MED- 54	• Medication Record Type
MED- 55	• Medication Dosing Status
MED- 56	• Medication Record Effective Start Date
MED- 57	• Medication Record Effective End Date
MED- 58	The component shall have the ability to return to a PHA a specified *subset* of the attributes of the medication record(s) for a specified patient. The specified subset may include any combination of the available attributes.
MED- 59	When modifying an existing medication record, the component shall have the ability to either (1) receive from a PHA only those fields that have been modified, and set the values of those fields to the received values, or (2) receive from a PHA an entire updated medication record, analyze which fields within the record have changed, and update only the changed fields to their new values.

Requirements Questions

Req ID or Section	Question
MED-31 to 43	Q: Should there be a minimum degree of structure and coding required for medication records in the med list CPC, i.e., such that PHAs cannot even store medication records that are not structured and coded to the minimum degree (put another way, which of the attributes of medication records should be required)? Or, should the CPC only specify the structure and code systems to be used when the PHAs are willing/able to structure and code medication data, but allow PHAs to not structure/code medication data if they wish? A: NO, the component should enforce minimal requirements with respect to which attributes are required to be populated, which fields must be coded, and which coding systems may be used. The technical specifications for the component should only "suggest" which attributes are required to be populated and/or coded, and which coding systems should be used.

5. Calendaring

Many PHAs require a calendaring component to help them record, track, share, and remind patients of specific scheduled events, tasks, or goals that are relevant to the management of their health or medical conditions. These scheduled events range from medical activities, such as a physician appointment or taking a medication, to personal activities, such as exercising, attending school, or taking a trip. The common platform component for calendaring (CP:CAL) must support the calendaring tasks of a variety of PHAs and must provide a common data model that enables multiple PHAs to share a single patient's calendar data.

5.1. PHAs and Calendaring

Table 5.1 lists the a number of functions related to calendaring that at least some of the PHAs under development in Project HealthDesign will seek to provide. These functions drive the specific requirements for the calendaring component, as described in the subsequent sections.

Table 5.1. PHA functions that require calendaring

No.	Function
1	Store and display the individual dates and times at which a patient should take a specific medication. This function helps patients who take multiple medications and/or medications with complex dosing regimens to keep track of when and how to administer their medications.
2	Store and display the dates and times at which a patient has scheduled various activities related to their health and wellness, such as medical appointments, physical exercise, meals, sleep, etc. This function helps patients to keep track of their other activities, as well as share their schedule of health-related activities with their healthcare providers, family members, and others.
3	Store and display complex treatment plans for specific illnesses, such as breast cancer, which consist of numerous tests and treatments scheduled over many months. This function helps patients to understand and follow their entire treatment regimen.
4	Store and display the dates and times at which a patient has scheduled personal activities that influence or constrain the planning of their health-related activities. Relevant personal activities may include going to work, attending school, traveling out of town, attending a social event, etc. This information helps patients and their healthcare providers to plan individual health-related events or a schedule of several health-related events.
5	Maintain a calendar that integrates all aspects of a patient's life, including their medical, professional, and personal plans in both the near term and the long term; display this "timeline" information to patients in creative ways that helps them to understand the context for the planned events in their lives and to manage the various aspects of their lives effectively.
6	Help patients to keep track of health-related goals and "to-do" tasks that have associated deadlines, such as the goal to exercise three times within the next week, the goal to receive a flu vaccination by a particular date, or the task to record entries in a pain diary at least once per day.

7	Actively remind patients to "fulfill" scheduled events or goals related to their health and well being, such as taking a medication, keeping a medical appointment, exercising, or recording their blood glucose level. Reminders may be sent prior to the scheduled time of an event or task to encourage its timely fulfillment and/or after the scheduled time to alert a patient that it is "past due."
8	Based on the dosing instructions in a patient's medication prescription and on the patient's schedule of existing activities, assist a patient or caregiver to *manually generate* a detailed schedule of the dates/times at which the patient should take the medication.
9	Based on the dosing instructions in a patient's medication prescription and on the patient's schedule of personal activities, *automatically generate* a detailed schedule of the dates/times at which the patient should take the medication.
10	Allow other persons beside the patient to view and comment upon the patient's schedule of health-related events and those personal events that influence their health or well being.

5.2. Sources of Data for Calendars in Personal Health Records

The calendaring component of a PHA will collect data in a number of ways, and the requirements for the component must reflect and accommodate each of these methods. Table 5.2 lists the various ways that calendar data may be populated, as expressed by the grantees of Project HealthDesign.

Table 5.2. Requirements for Calendaring Common Platform Component: Data Sources

Req ID	Requirement
CAL- 1	The Calendar component shall have the ability to store events and related reminders that are entered manually by the patient, a family member, a caregiver, or a healthcare provider in a manner controlled by a PHA.
CAL- 2	The Calendar component shall have the ability to store medical-appointment events that are imported from external scheduling applications, such as those used by a health-care facility.
CAL- 3	The Calendar component shall have the ability to store personal events and related reminders that are imported from an alternative personal calendar system (E.g., Outlook, Google, etc.) that may be used by a patient
CAL- 4	The Calendar component shall have the ability to store events and related reminders that are generated automatically by a PHA (for example, an automatically generated dosing schedule for a specific medication, an automatically generated exercise schedule, or an automatically generated schedule for patients to record observations regarding their condition).

5.3. Data Model for the Calendaring Platform Component

The calendar component shall manage and process three types of objects: *Calendar Events, Calendar Tasks,* and *Calendar Reminder*s. Calendar events are the scheduled activities that populate a calendar. Calendar tasks are "To-do" items associated with a deadline. Calendar reminders are timed messages associated with calendar events or calendar tasks that remind patients of the events/tasks or provide useful

information prior to or after them. The following sections describe the requirements for calendar events, calendar tasks, and calendar reminders.

Note: The calendar component, as conceptualized in this document, is not intended to store and manage records of *historical events*, i.e., the actual occurrences of planned activities, such as the taking of a medication, the performance of a physical activity, or the recording of a physiological parameter. These historical events are recorded within the Observations Component (see Section 6). Under this model, a PHA that needs to process or display past and future events together shall need to access both the calendar component and the observations component. Certain associations between the two components are included in the data model of the calendar component (such as references to the observations that fulfilled scheduled events), but the components are generally independent.

5.3.1. Types of Calendar Events

The data model of the calendaring component shall explicitly distinguish different types of calendaring events, so as to enable access control, selective data retrieval, and data export based on these event types. Table 5.3 lists the types of calendar events that the calendar component shall support.

Table 5.3. Types of Calendar Events

Req ID	Requirement
	The calendaring component shall have the ability to store and distinguish among the following types of calendar events:
CAL- 5	• Medication administration event [i.e., the time at which or time window during which a specific medication should be taken by or administered to the patient outside of an encounter with a healthcare professional]
CAL- 6	• Medical appointment event [i.e., the scheduled date/time of various encounters with healthcare professionals for diagnostic, therapeutic, or consultative purposes. These may include office visits, encounters for diagnostic and therapeutic procedures, and telephone/telemedicine consultations]
CAL- 7	• Observation recording event [i.e., the date/time at which the patient should record an observation or set of observations in the course of daily living (i.e., outside of an encounter with a healthcare professional). Examples of observation recording events include recording a blood glucose measurement, uploading data from an activity monitor, or making an entry in a pain log.]
CAL- 8	• Physical exercise event [i.e., the date/time at which or date/time window during which a specific physical exercise event is scheduled to occur]
CAL- 9	• Meal/snack event [i.e., the date/time at which a meal or snack is typically consumed or is planned to be consumed. This information is useful, for example, for the automated scheduling of medication-administration events that involve meals and food]

CAL- 10	• Sleep event [i.e., the time window during which overnight sleep or daytime sleep typically occurs. This information is useful for the automated scheduling of medication-administration events that should occur upon waking or prior to sleeping, as well as to avoid the scheduling of medication administration events during sleep]
CAL- 11	• School/work event [i.e., the time window during which the patient is away from his home at school or work. This information is useful for planning medication-administration events based on the environment in which the patient will be.]
CAL- 12	• Personal event [i.e., the date/time at which or time window during which a non-medical event is scheduled to take place; this type will be used to categorize non-medical events that do not fall into one of the other categories, such as social events, travel, hobbies, etc.]
CAL- 13	• Medical event [i.e., the date/time at which or time window during which a medical event is scheduled to take place; this type will be used to categorize medical events that do not fall into one of the other categories, such as prescription refills, self-administered therapies, etc.]
CAL- 14	• ~~"Deadline" event~~ ~~[Note: This special type of event records the date/time by which some action(s) should occur, although the action(s) may take place at any point prior to the deadline. Deadline events are useful for recording health-related goals and "To-do" items that entail deadlines, but not specific times (such as "exercise 3 times before next Sunday" or "get flu vaccine by Nov. 1".]~~ *Requirement Deleted.* "Deadline events" are now represented by Calendar Tasks (see Section 5.3.4)
	(intentionally empty)
CAL- 15	The set of event types supported by the calendaring component shall be extensible, so that new or unanticipated types of events may be recorded and processed by the component when required by PHAs.

5.3.2. Attributes of Calendar Events

Based on the intended functions, sources of data, and types of events that the calendar component is required to support, calendar events shall consist of the data attributes listed in Table 5.4.

Table 5.4. Attributes of Calendar Events

Req ID	Requirement
	For each event in the calendar, the calendar component shall be able to store the following data elements:
CAL- 16	• Calendar Event Unique ID (text) [Note: Assigned automatically by calendar component]

CAL- 17	• Patient Record ID (text) [Note: this attribute stores the unique identifier of the patient record to which this calendar event applies.]
CAL- 18	• Calendar Event Type (code) [E.g., "E-08" {code = "Physical Exercise"}; i.e., one of the observations types defined by the common platform data model, such as "meal/snack event", "medical event", etc.]
CAL-18.1	• Calendar Event Sub-Type (format TBD) [Note: PHAs may arbitrarily assign sub-types to calendar records to assist in the processing of calendar events. For example, a PHA may store additional structured data for a calendar event (i.e., data not defined by the common platform data model – see the Additional Structured Data attribute below), and the Sub-Type designator allows PHAs to retrieve and process calendar events specific to the sub-types that they have defined. The Sub-Type value must consist of a Sub-Type designator and the unique identifier of the PHA that created the observation record (to ensure uniqueness for the Sub-Type designators across PHAs)]
CAL- 19	• Short Text Label (text) [E.g., "Walking with Lynn"]
CAL- 20	• Long Text Description (text) [E.g., "Try to walk around the pond twice; stop after one lap if dizzy, short of breath or any leg pain; meet Lynn in parking lot"
CAL- 21	• Scheduled Event Start Time (formatted date/time) [E.g., "2007-11-07 16:00:00 GMT -0800"]
CAL- 22	• Scheduled Event End Time (formatted date/time) [E.g., "2007-11-07 17:30:00 GMT -0800"] (Note: if the event is scheduled to occur at a discrete time point, the Start Time and End Time may be the same.)
CAL- 23	• Estimated Scheduling Window (formatted date/time) [E.g., "2007-11-04 08:00:00 GMT -0800" TO "2007-11-11 18:00:00 GMT -0800"] (Note: This attribute is intended to capture a general time window during which an event will later be scheduled, although a specific time has not yet been determined. This attribute allows the calendar to store the range of time during which a significant future event *may* take place (such as a surgery, major social event, vacation, etc.), to assist in the planning of other medical and personal events affected by it.
CAL- 24	• Event Status (coded) [The allowed values = "Estimated", "Scheduled", "Cancelled", and "Fulfilled"] (Note: The "Fulfilled" value represents whether the scheduled event actually occurred. Depending on the design of the PHA and the type of event, this value may be set manually by a user, or it may be set automatically by the PHA, for example in response to a recorded observation, such as a blood glucose measurement).
CAL- 25	• Associated reminder(s) (format TBD) (Note: The set of reminders set for this event; see Section 5.3.7 for the data attributes of reminders).

CAL- 26	• Reference/link to the observation(s) that fulfilled the calendar event (format TBD) (Note: This attributes maintains a relationship between the scheduled event and one or more recorded observations that represent or describe the *actual* event [The common platform component for capturing and representing observations is described in Section 6]. For example, for a medication-administration event in the calendar, this attribute would reference the observation that describes when the medication was actually taken, how much was actually taken, etc. Also, for a deadline event such as "exercise 3 times by Sunday," this attribute would reference the recorded observations of the three exercise events that took place (i.e., their time, type, duration, intensity, etc.)
CAL- 27	• Reference/link to a data-entry form, application, or other mechanism for patients to record information associated with the fulfillment of the calendar event. (format TBD) (Note: This attribute will help a PHA identify and present the specific data-entry mechanism to be used to record observations related to the fulfillment of the calendar event. For example, the calendar event "Take Celebrex, 2 tablets" might be linked to a small data-entry form that allows the user to indicate the exact time at which they took the scheduled dose of Celebrex, how much was actually taken, and the reason for any deviation from the prescribed dosing. The values of this attribute and the data-entry forms used will probably be specific to individual PHAs.)
CAL- 28	• Annotations (text) [E.g., "We should discuss whether it's possible to schedule these workouts a little earlier, so they're closer to your last meal. - Carla, your diabetes care manager."] (Note: These annotations may be entered by other users, as permitted by the relevant access controls. Each annotation shall include a timestamp and the identity of the user who inserted it.)
CAL- 29	• Additional Structured Data (structured text) [Note: This attribute shall store an ASCII-encoded text blob (structured or unstructured) that may be inserted and accessed by one or more PHAs. The structure and/or coding used within this field (such as XML) shall be defined *ad hoc* by the PHAs that use the field; i.e., it will not be part of the data model of the calendar component itself.
CAL-29.1	• Reference/Link to Repeating Calendar Event (format TBD) [Note: When a Calendar Event is part of a set of repeating calendar events, as specified by a Repeating Calendar Event object (see Section 5.3.3), this attribute shall provide a "pointer" to the Repeating Calendar Event object. Referencing the Repeating Calendar Event object shall allow the PHA to display or update the repeating pattern.]
CAL-29.2	• Busy/Free Designation (coded) (Allowed values = "Busy" or "Free") [Note: This attribute shall designate whether the calendar event represents a period of time during which the record subject is available to fulfill other calendar events ("Free") or unavailable ("Busy"). This designation may assist in the manual or computer-assisted scheduling of other calendar events, for example when the text description of a scheduled event has been "blinded".]

	For each <u>Medication Administration Event</u> in the calendar, the calendar component shall be able to store the following data elements in addition to those already listed:
CAL- 30	• Reference/link to Medication-List entry (format TBD) [Note: This attribute shall be used to reference the medication-list entry (e.g., prescription or dispense record) that corresponds to the scheduled medication-administration event. Such a link will enable a PHA to display to users additional information regarding the medication that is scheduled to be taken (for example, an image of the pill, if the patient is unsure whether they are taking the right drug, or information about what to do if a dose is missed).
	For each <u>Medical Appointment Event</u> in the calendar, the calendar component shall be able to store the following data elements in addition to those already listed:
CAL- 31	• Electronic Contact Information (format TBD) [Note: This attribute will store a fax number, email address, web URL, or other electronic addressing information that a PHA can use to automatically transmit relevant data to the healthcare provider that the patient is scheduled to see. This convenience feature will allow blood glucose trends, pain diary entries, and other observations to be forwarded electronically to providers prior to medical appointments.]

5.3.3. Repeating Calendar Events

In addition to storing individual calendar events, the calendar component shall also store *repeating* calendar events. Repeating Calendar Events are aggregations of individual calendar events that may be created, modified, or deleted together. For example, a medical appointment that is scheduled to occur every Monday for a period of six weeks will be represented by six individual calendar events and one repeating calendar event that aggregates them.

Table 5.5. Attributes of Repeating Calendar Events

Req ID	Requirement
	For each repeating calendar event, the calendar component shall be able to store the following data elements:
CAL- 32	• Repeating Calendar Event Unique ID [Assigned automatically by the component]
CAL- 33	• Patient Record ID (text) [Note: this attribute stores the unique identifier of the patient record to which this repeating calendar event applies.]
CAL- 34	• Repeat frequency (format TBD) [E.g., “daily”, “weekly”, “every 3 weeks”, etc.]
CAL- 35	• Repeat End Time (formatted date/time) [E.g., “2007-11-07 24:00:00 GMT -0800”]
CAL- 36	• Reference/link to the set of individual calendar events in the repeating sequence (format TBD)

5.3.4. Types of Calendar Tasks

The data model of the calendaring component shall also explicitly distinguish different types of calendaring tasks. Calendar Tasks are distinct from Calendar Events in that they record the "deadline" by which some action(s) should occur, although the specific date and time of the action(s) is not specified. Calendar Tasks are useful for recording health-related goals and "To-do" items that entail deadlines, but not specific times (such as "exercise 3 times before next Sunday" or "get flu vaccine by Nov. 1"). The types of Calendar Tasks listed in Table 5.6 are similar to the types of Calendar Events, although certain types of Calendar Events are omitted because they are not applicable.

Table 5.6. Types of Calendar Tasks

Req ID	Requirement
	The calendaring component shall have the ability to store and distinguish among the following types of calendar tasks:
CAL-36.1	• Medication refill task [i.e., a goal or task related to the refilling of a medication prescription]
CAL-36.2	• Medical appointment task [i.e., a goal or task related to a medical appointment that has not been specifically scheduled, for example "get a physical exam by the end of the year"]
CAL-36.3	• Observation recording task [i.e., a goal or task related to the recording of an observation that has not been specifically scheduled. For example, "record weight at least once each week"]
CAL-36.4	• Physical exercise task [i.e., a goal or task related to physical exercise that has not been specifically scheduled. For example, "swim 3 times this week"]
CAL-36.5	• Meal/snack task [i.e., a goal or task related to the consumption of a meal or snack]
CAL-36.6	• Sleep task [i.e., a goal or task related to sleep]
CAL-36.7	• School/work task [i.e., a goal or task related to work or school]
CAL-36.8	• Personal task [i.e., a personal goal or task that is not otherwise covered by one of the other calendar task types]
CAL-36.9	• Medical task [i.e., a medical goal or task that is not otherwise covered by one of the other calendar task types]
	(intentionally empty)
CAL-36.10	The set of task types supported by the calendaring component shall be extensible, so that new or unanticipated types of events may be recorded and processed by the component when required by PHAs.

5.3.5. Attributes of Calendar Tasks

Based on the intended functions, sources of data, and types of events that the calendar component is required to support, calendar events shall consist of the data attributes listed in Table 5.7.

Table 5.7. Attributes of Calendar Tasks

Req ID	Requirement
	For each task in the calendar, the calendar component shall be able to store the following data elements:
CAL-36.11	• Calendar Task Unique ID (text) [Note: Assigned automatically by calendar component]
CAL-36.12	• Patient Record ID (text) [Note: this attribute stores the unique identifier of the patient record to which this calendar event applies.]
CAL-36.13	• Calendar Task Type (code) [E.g., "T-08" {code = "Medication Refill"}; i.e., one of the task types defined by the common platform data model, such as "physical exercise", etc.]
CAL-36.14	• Calendar Task Sub-Type (format TBD) [Note: PHAs may arbitrarily assign sub-types to calendar task records to assist in the processing of calendar tasks. For example, a PHA may store additional structured data for a calendar task (i.e., data not defined by the common platform data model – see the Additional Structured Data attribute below), and the Sub-Type designator allows PHAs to retrieve and process calendar tasks specific to the sub-types that they have defined. The Sub-Type value must consist of a Sub-Type designator and the unique identifier of the PHA that created the observation record (to ensure uniqueness for the Sub-Type designators across PHAs)]
CAL-36.15	• Short Text Label (text) [E.g., "Get flu vaccination"]
CAL-36.16	• Long Text Description (text) [E.g., "Ask Dr. Quincy where it's most cost-effective to get the vaccine. Maybe go together with Dorothy"
CAL-36.17	• Scheduled Task Start Time (formatted date/time) [E.g., "2007-11-07 16:00:00 GMT -0800"] (Note: This attribute, when populated, will denote the beginning of the period during which the task should be completed. For example, if a patient should exercise at least three times each week, the task start time will be the first day of the week, so that the PHA may keep track of the interval during which exercise events are "counted" towards fulfilling the task)
CAL-36.18	• Scheduled Task End Time (formatted date/time) [E.g., "2007-11-07 17:30:00 GMT -0800"] (Note: This attribute denotes the deadline by which the task should be completed)

CAL-36.19	• Task Status (coded) [The allowed values = "Scheduled", "Cancelled", and "Fulfilled"] (Note: The "Fulfilled" value represents whether the goal was met or the task performed. Depending on the design of the PHA and the type of task, this value may be set manually by a user, or it may be set automatically by the PHA, for example in response to a recorded observation, such as an exercise event).
CAL-36.20	• Associated reminder(s) (format TBD) (Note: The set of reminders set for this task; a Calendar Task may have the same type(s) of reminders as a Calendar Event see Section 5.3.7 for the data attributes of reminders).
CAL-36.21	• Reference/link to the observation(s) that fulfilled the calendar task (format TBD) (Note: This attributes maintains a relationship between the scheduled event and one or more recorded observations that represent or describe the *actual* event [The common platform component for capturing and representing observations is described in Section 6]. For example, for a goal such as "exercise 3 times by Sunday," this attribute would reference the recorded observations of the three exercise events that took place (i.e., their time, type, duration, intensity, etc.)
CAL-36.22	• Reference/link to a data-entry form, application, or other mechanism for patients to record information associated with the fulfillment of the calendar task. (format TBD) (Note: This attribute will help a PHA identify and present the specific data-entry mechanism to be used to record observations related to the fulfillment of the calendar task. For example, the calendar task "Get flu vaccination" might be linked to a small data-entry form that allows the user to indicate the exact date and place at which she received the vaccination The values of this attribute and the data-entry forms used will probably be specific to individual PHAs.)
CAL-36.23	• Annotations (text) [E.g., "Losing 20 pounds in 6 weeks might be a little too ambitious. Let's discuss. - Carla, your diabetes care manager."] (Note: These annotations may be entered by other users, as permitted by the relevant access controls. Each annotation shall include a timestamp and the identity of the user who inserted it.)
CAL-36.24	• Additional Structured Data (structured text) [Note: This attribute shall store an ASCII-encoded text blob (structured or unstructured) that may be inserted and accessed by one or more PHAs. The structure and/or coding used within this field (such as XML) shall be defined *ad hoc* by the PHAs that use the field; i.e., it will not be part of the data model of the calendar component itself.

5.3.6. Types of Calendar Reminders

Calendar reminders are instructions associated with a calendar event or a calendar reminder to message a specified user in a specified way at a specified time interval before or after the event. Although reminders are always attributes of a calendar event, they are sufficiently complex that we describe the types of reminders and their data attributes separately below.

Table 5.8. Types of Calendar Reminders

Req ID	Requirement
	The calendaring component shall have the ability to store and process the following types of calendar reminders:
CAL- 37	"Prompt" Reminder: A reminder that is issued at a specified time interval *prior* to the Start Time of a scheduled event or the deadline of a task. The purpose is to gently remind a user that the event or deadline is forthcoming.
CAL- 38	• If the event/task is fulfilled prior to the time that a prompt reminder is issued, the reminder is automatically cancelled.
CAL- 39	• A prompt reminder may be issued only once; if multiple reminders at different time intervals prior to an event/tasks are desired, each must be specified as a separate reminder
CAL- 40	"Nag" Reminder: A reminder that is issued at a specified interval *after* the Start Time or the End Time of a scheduled event or after the deadline of a scheduled task if the event/task has not yet been fulfilled. The purpose is to inform a user that the event or task is "past due." (Note: A Nag Reminder may also be used to instruct a user to *not* fulfill a scheduled event or event if they have not done so within a specific interval of its scheduled time; for example, if the dosing time of a medication is missed, the patient may be instructed to wait until the next scheduled dose rather than take the medication late.)
CAL- 41	• If the event is fulfilled prior to the time that the nag is issued, the nag is automatically cancelled.
CAL- 42	• ~~If the event remains unfulfilled for a specified time interval after the nag is issued, the same nag may be re-issued or it may be "escalated", i.e., sent via a different channel or to a different user~~ *Original Requirement Deleted.* If there is a wish to have "escalating" reminders, multiple reminders shall be specified, each scheduled at an increasing time interval.
CAL- 43	• ~~If the reminder remains unacknowledged for a specified time interval after the reminder is issued, the same reminder may be re-issued or it may be "escalated", i.e., sent via a different channel or to a different user~~ *Original Requirement Deleted.* If there is a wish to have "escalating" reminders, multiple reminders shall be specified, each scheduled at an increasing time interval
CAL- 44	"Informational" Reminder: The calendaring component shall have the ability to store and process a reminder that is issued at a specified interval *before or after* a scheduled event or task. The purpose is to provide helpful information related to a calendared event/task at an appropriate time relative to that event. For example, a patient may be reminded to fast 12 hours prior to a diagnostic test or to check their blood glucose 10 minutes following a scheduled physical activity.
CAL- 45	• If the associated event is fulfilled prior to the time that the informational reminder is issued, the reminder may still be issued (depending on the behavior specified when the reminder is created).

5.3.7. Attributes of Calendar Reminders

Table 5.9. Attributes of Calendar Reminders

Req ID	Requirement
	For each reminder in the calendar, the calendar component shall be able to store the following data elements:
CAL- 46	• Calendar Reminder Unique ID (text) [Note: The component shall assign a *Calendar Reminder Unique ID* to each distinct calendar reminder. A PHA can later use this identifier to reference a specific calendar reminder.]
CAL- 47	• Patient Record ID (text) [Note: this attribute stores the unique identifier of the patient record to which this calendar reminder applies.]
CAL- 48	• Calendar Reminder Type (code) [E.g., "R-08" {code = "Prompt"}] (Note: The reminder type will determine the appropriate behavior for each calendar reminder. For example, a nag reminder will be cancelled once the event/task is fulfilled, whereas an informational reminder may still be executed.)
CAL- 49	• Reference/link to the scheduled event/task with which the reminder is associated (format TBD)
CAL- 50	• Indicator whether the reminder should be executed at a time relative to the Start Time or End Time of the calendar event/task (coded) [Allowed values = "Start" or "End"]
CAL- 51	• Time period before or after the associated calendar event/task at which the reminder should be executed (formatted as Days:Hours:Minutes) [E.g., "00:12:00" = 12 hours after, "-02:00:00" = 2 days before] (Note: The value may be positive or negative)
CAL- 52	• Currently Scheduled Execution Time (formatted date/time) [E.g., "2007-11-07 1530:00:00 GMT -0800"] (Note: This attribute represents the absolute date/time at which the reminder is currently scheduled to execute. This shall be a read-only attribute, as its value is always computed based on the schedule of the associated calendar event and the specified offset of the reminder from that time.)
CAL- 53	• Method for delivering the reminder (coded) [Allowed values = "PHA Messaging", "Email", "SMS", "Phone", "Per PHA Preference", "Per User Preference"] (Note: "Per PHA Preference" = the PHA will dynamically determine the delivery method based on its own logic (which may include any user preferences that the PHA has stored); "Per User Preference" = the PHA will deliver the reminder based on the delivery method specified by the user *within the calendaring component*. This feature allows a user to specify a notification method across several PHAs that use the same calendar component.)

CAL- 54	• Recipient of the reminder (User ID as text) (Note: A single recipient is specified for each reminder. This is required to support the tracking of reminder acknowledgement. If a single reminder is to be sent to multiple recipients, multiple calendar reminder instances are required)
CAL- 55	• Reminder Message Source (coded) [Allowed values = "Hard Coded" or "Per PHA Preference"] (Note: "Hard-Coded" = the reminder message is the value of the Reminder Message Content attribute (see below) "Per PHA Preference" = the PHA will dynamically determine the content of the reminder message based on the calendar event type, specific calendar event, duration since scheduled time of the event, etc..)
CAL- 56	• Reminder Message Content (MIME-encoded text) [Should leverage MIME encoding that allows content to be sent as both plain text and HTML] (Note: May only be empty if the Reminder Message Source attribute = "Per PHA Preference")
CAL- 57	• Reminder Status (coded) [Allowed values = "Set", "Cancelled", "Executed", "Acknowledged"] (Note: Set = the reminder is set to execute at the specified time Cancelled = the reminder has been cancelled and will not execute Executed = the reminder has been sent to the specified recipient Acknowledged = the specified recipient has acknowledged receipt of the reminder)

5.4. Required Functionality for the Calendaring Platform Component

Table 5.10 lists the specific functions and operations that the calendaring component shall be able to perform.

Table 5.10. Required Functionality for the Calendaring Platform Component

Req ID	Requirement
CAL- 58	The component shall have the ability to *insert a new calendar event or task* into the calendar for an existing patient when a PHA supplies all of the required attribute values and represents all attribute values using allowed formats and coding systems.
CAL- 59	The component shall have the ability to *modify an existing calendar event or task* (as referenced by its Unique ID) when a PHA represents all of the updated attribute values using allowed formats and coding systems.
CAL- 60	The component shall have the ability to *delete an existing calendar event or task* (as referenced by its Unique ID)
CAL- 61	The component shall have the ability to *insert a new calendar reminder* into the calendar for an existing calendar event or task (as referenced by its Unique ID) when a PHA supplies all of the required attribute values and represents all attribute values using the allowed formats and coding systems.

CAL- 62	The component shall have the ability to *modify an existing calendar reminder* (as referenced by its Calendar Reminder Unique ID) when a PHA represents all of the updated attribute values using the allowed formats and coding systems.
CAL- 63	The component shall have the ability to *delete an existing calendar reminder* (as referenced by its Calendar Reminder Unique ID)
CAL- 64	The component shall make all modifications to and deletions of existing calendar events, tasks, and reminders "non-destructively," i.e., a record of the previous values of any modified or deleted medication records will be retained within the system, along with a record of when the modification/deletion occurred and which user requested it (see Audit Logging in Section 7.5).
CAL- 65	The component shall maintain the specified temporal relationship between a calendar event/task and its associated calendar reminders when the scheduled time of a calendar event/task is modified.
CAL- 66	The component shall not enforce any temporal constraints for medication administration events that are implied by the corresponding medication-list records (i.e., prescriptions). Specifically, the component shall allow authorized users to make any changes to medication administration records, even if those changes are inconsistent with a medication prescription.
CAL- 67	The component shall have the ability to retrieve and return to a PHA all attributes of all the calendar events/tasks for a specified patient in a single operation
	The CPC shall have the ability to return to a PHA a subset of the calendar events/tasks for a specified patient based on a query expression that includes comparisons (>, <, =, LIKE) and Boolean combinations (AND, OR, NOT) involving the following attributes:
CAL- 68	• Calendar Event/Task Unique ID
CAL- 69	• Calendar Event/Task Type
CAL- 69.1	• Calendar Event/Task Subtype
CAL- 70	• Short Text Label
CAL-70.1	• Long Text Label [to enable ability to search for an event based on its long label]
CAL- 71	• Scheduled Event/Task Start Time
CAL- 72	• Scheduled Event/Task End Time
CAL- 73	• Estimated Scheduling Window Start Time (for Events only)
CAL- 74	• Estimated Scheduling Window End Time (for Events only)
CAL- 75	• Event/Task Status
CAL- 76	The CPC shall have the ability to return to a PHA a specified *subset* of the attributes of the calendar event(s)/task(s) for a specified patient. The specified subset may include any combination of the available attributes.

	The CPC shall have the ability to return to a PHA a subset of all calendar reminders based on query expressions that include comparisons (>, <, =) and Boolean combinations (AND, OR, NOT) involving the following attributes:
CAL- 77	• Patient Record Unique ID (i.e., the identifier of a specific patient, if desired. Otherwise, the component shall return *all* of the reminders that meet the other query criteria)
CAL- 78	• Calendar Reminder Unique ID
CAL- 79	• Associated Calendar Event/Task Unique ID (i.e., the event/task for which the reminder exists)
CAL- 80	• Reminder Status
CAL- 81	• Currently Scheduled Execution Time
CAL- 82	The component shall allow a PHA to *subscribe to reminder events* for specific patients, such that when the time at which a reminder should be executed is reached, the component shall automatically notify the PHA and transmit the corresponding reminder data to the PHA.
CAL- 83	The component shall have the ability to *import calendar events and tasks* from other calendaring applications (such as Outlook, Google, etc.). The import function shall be configurable, such that a user may select the date-range of events to be imported. The import function shall allow a user to "mask" or modify the descriptions for any calendar events that are imported from another calendar, to protect privacy (for example, change the label of every imported event to "personal commitment").
CAL- 84	The component shall have the ability to *export calendar events and tasks* to other calendaring applications (such as Outlook, Google, etc.). This export function shall be configurable, such that a user may select the type(s) of events to be exported and/or the date-range of events to be exported. The component will export all attributes of calendar events that can be supported by the target calendaring system (for example, the date/time, label, and "prompt" reminders). The export function shall allow a user to "mask" or modify the descriptions for any calendar events that are exported to another calendar, to protect privacy (for example, change the label for any event of the type Medical Appointment from the specific "chemotherapy" or "mammogram" to the generic "Medical Appointment").
CAL- 85	The component shall have the ability to *synchronize calendar events and tasks* with another calendaring applications, such that events added or changed in one calendar shall be automatically propagated to the other. Synchronization between the component and another calendar application may require certain constraints, so that the personal health record calendar remains the "source of truth" for health-related events.
CAL- 86	When modifying an existing calendar event, task, or reminder, the component shall have the ability to either (1) receive from a PHA only those fields that have been modified, and set the values of those fields to the received values, or (2) receive from a PHA an entire updated calendar event, task, or reminder record, analyze which fields within the record have changed, and update only the changed fields to their new values.

Requirements Questions

Req ID or Section	Question
	Q: When updating calendar events and calendar reminders, should the API include a function that allows an entire cached med-list record to be re-inserted such that the component figures out which (if any) attributes were updated and appropriately updates just those? This is versus a more "piecemeal" approach in which the PHA has to know which values it has changed and only updates those attributes selectively. A: YES [see Requirement CAL- 86]

6. Observations Captured in the Course of Daily Living

Patients use PHRs to document the signs and symptoms of their health conditions and to log their health-related activities in the course of daily living, i.e., outside of their physician visits, hospital stays, and other encounters with the health care system. A record of health-related observations captured in the course of daily living can be a valuable resource to help patients track and manage their own illnesses, to help health care providers monitor and better treat their patients, and to help patients and their health care providers collaborate in their care more effectively.

There are two general types of observations that are useful for patients to record in the course of daily living:

1. Actions performed by or on the patient: For example, a medication administration, the ingestion of a meal, participation in an exercise activity, etc.
2. Subjective or objective characteristics of the patient's state: For example, a glucose measurement, a blood-pressure reading, the sensation of pain, the perception of mood, the appearance of a rash

This section describes the requirements for a common platform component for recording and managing such observations (CP:OBS).

Note: PHRs and PHAs need to include other medical information that is typically recorded during interactions with the health care system, such as a problem list, surgical history, vaccination history, and results of laboratory tests and imaging studies. Although it is often important to store, display, and process these data in PHRs and PHAs, the requirements for doing so are not included here because these types of observations are not captured in the course of daily living. Also, electronic health record systems have already developed models for processing these types of data, which may be applied within a common platform for personal health record storage or within individual PHAs.

6.1. PHAs and Observations

Table 6.1 lists a number of functions related to the recording of observations that at least some of the PHAs under development in Project HealthDesign may need to perform. These functions drive the specific requirements for the observations component, as described in the subsequent sections.

Table 6.1. PHA functions that require a record of observations

No.	Function
1	Graph related observations against each other to visually display the relationships and possibly identify causal patterns (for example, blood glucose level vs. insulin dosing vs. food ingestion vs. physical activity OR pain-medication dosing vs. physical activity vs. pain)
2	Enable patients to log their "fulfillment" of calendar events (e.g., taking medications, exercise, etc.) to help patients adhere to an appropriate schedule by tracking the intended time of an action versus whether and when the action actually took place.
3	Enable patients to record and track the subjective and objective indicators of their condition (e.g., blood glucose, blood pressure, pain, mood) and communicate to their health care professionals trends or variations in these indicators that occur between office visits
4	Enable patients to record and track their health-related actions between physician visits (e.g., medication administration, meals, physical activity) and communicate to their health care professionals the relevant specifics of these actions (e.g., the specific nutritional content of meals or the specific frequency, intensity and duration of physical exercise)
5	Notify caregivers or healthcare professionals when certain observations are recorded by a patient. For example, notify a diabetes care manager each time a patient uploads her glucose meter readings, so that the care manager may review them, or notify the care manager only when a patient uploads readings above a specified threshold.
6	Analyze relevant observation data to automatically make recommendations to patients regarding the management of their conditions or to automatically assess the impact of changes that patients are considering ("what-if" analysis). Recommendations may address, for example, an appropriate exercise plan, appropriate meals to eat, or the appropriate schedule for administering pain meds.

6.2. Sources of Observations in Personal Health Records

The observations component of a PHA will collect data in a number of ways, and the requirements for the component must reflect and accommodate each of these methods. Table 6.2 lists the various ways that observation data may be populated, as expressed by the grantees of Project HealthDesign.

Table 6.2. Requirements for Observation Common Platform Component: Data Sources

Req ID	Requirement
OBS- 1	The component shall have the ability to store observations that have been manually entered by a patient or caregiver as *structured data elements* (presumably via a structured data-entry form provided by a PHA). [E.g., a structured blood glucose reading with coded units, the coded representation of a symptom or physical sign, the coded representation of a physical exercise activity, etc.]

OBS- 2	The component shall have the ability to store observations that have been manually entered by a patient or caregiver via a PHA as responses to a *pre-defined questionnaire or survey instrument*. [E.g., responses to a depression-scale questionnaire, selection of "other" in response to a multiple-choice survey questions, free-text responses in questionnaires, etc.]
OBS- 3	The component shall have the ability to store observations that have been manually entered by a patient or caregiver as *unstructured text notes, blogs, or journal entries*
OBS- 4	The component shall have the ability to store observations that have been electronically uploaded from a *measurement device* via a PHA-mediated interface. [E.g., a glucometer, pedometer, or accelerometer]
OBS- 5	The component shall have the ability to store observations that have been electronically uploaded as *photographs or other image files* [E.g., the photograph of a meal, an emoticon depicting a patient's mood, a scanned drawing depicting a patient's mood]

6.3. Data Model for the Observations Platform Component

The great variety of observations that may be recorded in a personal health record presents a challenge for the design of a data model for the observations platform component. Additionally, the variable need for structure and coding of observations across different PHAs creates a trade-off: Allowing PHAs to record observation data at whatever level of structure/coding they require enables the broadest range of PHAs to benefit from the CP:OBS component, but limits the sharing of data across PHAs with different structure and coding needs. The requirements documented here attempt a compromise between the goals of widespread applicability on one hand and PHA-to-PHA interoperability on the other. The requirements specify significant structure and coding for certain types of observations when such structure/coding has been expressed as a requirement by the Project HealthDesign grantees. At the same time, the requirements allow other types of observations to be represented in whatever data formats suit the PHAs that capture them.

The sections below list the types of observations that the CP:OBS component can accommodate, the general attributes shared by all observation types, and the attributes specific to certain observation types. The requirements for a terminology system to represent the instances of specific observations in a consistently coded form is also described.

6.3.1. Types of Observations Records

Table 6.3. Types of Observation Records

Req ID	Requirement
	The component shall have the ability to store and distinguish among the following types of observation events:
OBS- 6	• Medication administration [i.e., the occurrence of a medication being taken or administered, including the time at which it took place and the details of the dosing]
OBS- 7	• Physical Activity [i.e., the structured description of a physical activity as entered by a user, including the type of activity, duration, intensity, etc.]

OBS- 8	• Meal/Snack [i.e., the time and characteristics of an ingested meal or snack, including the composition of the meal and/or a photograph of the food items]
OBS- 9	• Healthcare Encounter [i.e., an encounter with the healthcare system, such as a physician office visit, hospitalization, phone consultation, etc.]
OBS- 10	• Sign or Symptom [The presence or absence of a discrete sign or symptom, such as "fever", "fatigue", "nausea", "swelling", etc.; only the presence or absence of the sign or symptom can be described using this type of observation – no qualifiers are supported]
OBS- 11	• Pain [A sub-type of the Sign or Symptom type that allows a relevant set of pain qualifiers to be recorded, including location, severity, quality, radiation, etc.]
OBS- 12	• Observable Parameter [an "attribute/value" observation consisting of some observable parameter (such as systolic blood pressure) and the value of that parameter (such as "120 mmHg"); Note: The Observable Value type may be used to represent, among other things, the individual measurements captured by activity monitors.]
OBS-12.1	• Journal Entry [An unstructured text entry that captures a user's general subjective observations; may be a diary entry, a blog entry, etc.]
OBS- 13	• General Observation [A "catch-all" observation type that allows other types of observations to be represented per the structure and coding specifications of individual PHAs]
	(Intentionally empty)
OBS- 14	The set of event types supported by the calendaring component shall be extensible, so that new or unanticipated types of events may be recorded and processed by the component when required by PHAs.

6.3.2. Attributes of Observation Records

Based on the intended functions, sources of data, and types of records that the CP:OBS component is required to support, observation records shall consist of the *combination* of the data attributes described in Section 6.3.2.1 and the relevant attributes in Sections 6.3.2.2 - 6.3.2.9 (depending of the type of observation recorded).

6.3.2.1. Common Attributes

The attributes in Table 6.4 apply to observations of any observation type. Attributes specific to individual observation types are listed in the subsequent sections.

Table 6.4. Common Attributes of Observations

Req ID	Requirement
	For each observation record, the CP:OBS component shall be able to store the following data elements
OBS- 15	• Observation Unique ID (text) [Note: The component shall assign a *Observation Unique ID* to each distinct observation record. A PHA can later use this identifier to reference a specific observation.]
OBS- 16	• Patient Record ID (text) [Note: this attribute stores the unique identifier of the patient record to which this observation applies.]
OBS- 17	• Observation Type (coded) [i.e., one of the observations types defined by the common platform data model, such as "medication administration", "meal/snack", "pain", etc.]
OBS- 18	• Observation Sub-Type (format TBD) [Note: PHAs may arbitrarily assign sub-types to observation records to assist in the processing of observations. For example, a PHA may store additional structured data for an observation (i.e., data not defined by the common platform data model – see the Additional Structured Data attribute below), and the Sub-Type designator allows PHAs to retrieve and process observations specific to the sub-types that they have defined. The Sub-Type value must consist of a Sub-Type designator and the unique identifier of the PHA that created the observation record (to ensure uniqueness for the Sub-Type designators across PHAs)]
OBS- 19	• Observation Entry Datetime (formatted Date/Time) [E.g., "2007-11-09 21:14:33 GMT -0800"] (Note: This attribute represents the date/time at which the observation was recorded in the CP:OBS database)
OBS- 20	• Observation Effective Start Datetime (formatted Date/Time) [E.g., "2007-11-07 15:00:00 GMT -0800"] (Note: represents the beginning of the time interval at which the recorded action, symptom, medical appointment, etc. actually took place)
OBS- 21	• Observation Effective End Datetime (formatted Date/Time) (Note: represents the end of the time interval at which the recorded action, symptom, medical appointment, etc. actually took place. For observations occurring at a single point in time, this value may be equal to Observation Effective Start Datetime)
OBS- 22	• Text Comment/Description (text) [Note: stores an arbitrary text comment typically made by the recorder of the observation. For example, a brief note explaining why a medication was taken outside of its regularly scheduled dose, or why the patient visited the emergency room. This comment field is distinct from an "annotation" (see below), which is not an attribute of the observation, per se, but may be added to an observation by any authorized user. The separate treatment of annotations is required for access control purposes]

OBS- 23	• Annotations (text) [E.g., "This value is a little high. Please contact me if this doesn't go back below 150. – Dr. Grayson"] (Note: These annotations may be entered by other users, as permitted by the relevant access controls. Each annotation shall include a timestamp and the identity of the user who inserted it.)
OBS- 24	• Reference/Link to associated calendar event (format TBD) [Note: This attribute applies when an observation records an action that fulfilled or helped to fulfill a calendar event, such as a scheduled medication administration or exercise session; the attribute is populated at the discretion of the PHA (i.e., it is not maintained by the CP:OBS component).]
	• Reference/Link to associated Observation record (format TBD) [Note: this may be useful, for example, to relate the systolic and diastolic blood pressure readings of a single BP measurement.]
OBS- 25	• Additional Structured Data (XML text) [Note: This attribute can store additional information about an observation that a PHA wishes to store in a structured form, but is not accommodated by any of the existing structured attributes for the relevant observation type. For example, a PHA for breast cancer patients may wish to add structured information regarding the type of chemotherapy or radiation therapy administered during a medical appointment. Also, this field allows PHAs to store and process structured data for observation types that are not yet defined by the common platform data model. To do this, PHAs may specify a Observation Type of "General Observation" and create their own structured data model for representing the observation data.]
OBS-25.1	• Multi-media attachments (format type + content) [Note: This attribute may store one or more multi-media attachments of allowable format types (e.g., JPG, MPEG, etc. The set of types is TBD). A single observation may have multiple types of attachments (e.g., both a photo and an audio annotation).
OBS-25.2	• Provenance (code) (Values = "MedicalSource" "PersonalSource") [Note: This coded flag denotes whether the observation originated from an authorized and trusted medical source (such as directly from an EHR or laboratory) or whether it originated from a patient or other lay caregiver or custodian.]

6.3.2.2. Type-Specific Attributes: Medication Administration

Table 6.5. Attributes of Medication Administration Observations

Req ID	Requirement
	For each observation of type Medication Administration, the CPC shall be able to store the following data elements in addition to the general data attributes:
OBS- 26	• Medication Text (text) [Note: describes the medication administered, including route and dosage strength, if available]

OBS- 27	• Medication ID (code) [Note: If the CP:OBS component is used as a shared data repository, the same terminology model shall be used as for the CP:MED component; if the CP:OBS component is integrated into a specific PHA, the PHA may use whatever terminology it wishes (or no coded terminology) .]
OBS- 28	• Medication ID Code System (code) [Note: Identifies the terminology/coding system used for the Medication ID; for example, RxNorm, NDC, etc.]
OBS- 29	• Reference/Link to medication-list record (format TBD) [Note: Allows PHA to navigate to the associated medication-list record, as specified by the PHA that populates this observation record. Does not assume that the CP:MED component is used (a PHA may use another component or its own medication-list management module).]
OBS- 30	• Dose Amount Administered Value (number) [E.g., 2, 500]
OBS- 31	• Dose Amount Administered Units (coded) [E.g., mg, units] (Note: If the CP:OBS component is used as a shared data repository, the same terminology shall be used as for the CP:MED component)
OBS- 32	• Physical Quantity Administered Value (number) [E.g., 1. 2.5]
OBS- 33	• Physical Quantity Administered Units (coded) (Note: If the CP:OBS component is used as a shared data repository, the same terminology shall be used as for the CP:MED component)
OBS- 34	• Route of administration (text and coded) [E.g., oral, handheld injection, pump injection, transdermal] (Note: If the CP:OBS component is used as a shared data repository, the same terminology shall be used as for the CP:MED component)
OBS- 35	• Site of administration (text and coded) [E.g., thigh, shoulder for I.M. injection] (Note: this attribute may be relevant in cases when the site of administration affects the absorption rate of a medication)
OBS- 36	• Reason for administration (coded) [values = “scheduled administration”, “PRN”] (Note: Additional information regarding the reason for a PRN administration should be stored in the “Text Comment” attribute – see Table 6.4)

6.3.2.3. Type-Specific Attributes: Physical Activity – Described

Table 6.6. Attributes of Physical Activity

Req ID	Requirement
	For each observation of type Physical Activity – Described, the CPC shall be able to store the following data elements in addition to the general data attributes:
OBS- 37	• Activity Text (text) [e.g., “walking”, “biking”, “swimming”]
OBS- 38	• Activity ID (coded) [E.g., “875764993” {code = “swim”}]
OBS- 39	• Activity ID Code System (coded) [E.g., SNOMED]
OBS- 40	• Duration Text (text) [E.g., “30 minutes”, “2 hours”, “4 miles”]
OBS- 41	• Duration Value (number) [E.g., 30, 2]
OBS- 42	• Duration Units (coded) [codes = “minutes”, “hours”, “miles”]
OBS- 43	• Duration Units Code System (coded) [E.g., “SNOMED”]
OBS- 44	• Intensity Text (text) [E.g., “achieved max HR of 150”, “medium intensity”, “20 minutes before breaking a sweat”]
OBS- 45	• Intensity Value (text) [E.g., “150”, “medium”, “20”]
OBS- 46	• Intensity Units (coded) [e.g., max HR achieved, scale 1-10, enumerated{low,medium,high}, minutes before breaking a sweat, etc.]

6.3.2.4. Type-Specific Attributes: Meal/Snack

The composition Meals/Snacks may be recorded in a variety of ways by users, and this Type definition is intended to accommodate any of them. If the user enters only a free-text description of the meal, it shall be represented in the “Meal Text Description” attribute. If the user enters structured information separately recording the food type(s) and quantity(ies) eaten, the information shall be represented in the “Meal Text Description”, “Food Item ID”, and “Food Item Quantity” attributes. If the user specifies each constituent ingredient of a food item or an entire meal, this information may be placed in multiple values of the “Meal Ingredients” attribute.

Note: If a patient records only the text description of an entire meal, such as “16 oz Lasagna, large salad, glass of wine”, then this data shall be represented in the common attribute “Text Comment/Description”.

Table 6.7. Attributes of Meal/Snack Observations

Req ID	Requirement
	For each observation of type Meal/Snack, the CPC shall be able to store the following data elements in addition to those listed in Section 6.3.2.1:
OBS-46.1	• Meal/Snack Quantity (text) [E.g., "small", "3 large slices", "tall glass"
OBS- 47	• Food Items (zero to many values, structured) - Food Item Text (e.g., "Lasagna") - Food Item Code (E.g., "923847" {code = "Lasagna"}) - Food Item Coding System (E.g., "SNOMED") - Food Item Quantity (E.g. 16, "large", 2) - Food Item Quantity Units (E.g., oz, enumerated{small, medium, large}, count) - Food Item Quantity Units Coding System (E.g., "SNOMED") - Glycemic Index (integer)
OBS- 48	• Food Ingredients (zero to many values for each Food Item, structured) - Ingredient Text (E.g., "Pasta") - Ingredient Code (E.g., "5778" {code = "pasta"}) - Ingredient Quantity Value (E.g., "6") - Ingredient Quantity Units Text (E.g., "oz") - Ingredient Quantity Units Code (E.g., "5784" {code = "oz"}) - Ingredient Quantity Units Coding System (E.g., "SNOMED") - Glycemic Index (integer)
OBS- 49	• ~~Photo(s) of meal/snack (format TBD)~~ *Original Requirement Deleted.* Now handled by Requirement OBS-25.1

6.3.2.5. Type-Specific Attributes: Healthcare Encounter

Observations documenting healthcare encounters for patients may be recorded using only the common observation attributes listed in Section 6.3.2.1.

6.3.2.6. Type-Specific Attributes: Sign or Symptom

This observation type is intended to record the presence or absence of discrete signs and symptoms when structured information about the onset, duration, severity, and other qualifiers is not required (although this information may be recorded in an unstructured form in the Comment Text attribute or in a PHA-specific structured form in the Additional Structured Data attribute).

Note: This observation type is not intended to record observations represented as "attribute/value" pairs, such as "heart rate : 75", "blood glucose : 131", or "range of motion : 50%". The Observable Parameter observation type is intended for such observations (see Section 6.3.2.8).

Table 6.8. Attributes of Sign or Symptom Observations

Req ID	Requirement
	For each observation of type Sign or Symptom, the CPC shall be able to store the following data elements in addition to those listed in Section 6.3.2.1:
OBS- 50	• Symptom Text (text) [E.g., “fatigue”, “nausea”, “rash”, “palpitations”]
OBS- 51	• Symptom Code (text) [E.g., “868590388” {code = “fatigue”}]
OBS- 52	• Symptom Code Type (coded) [E.g., “SNOMED”, “UMLS”, “ICD-9”]
OBS- 53	• Status (coded) [values = “Present”, “Absent”, “Unknown”]

6.3.2.7. Type-Specific Attributes: Pain

Table 6.9. Attributes of Pain Observations

Req ID	Requirement
	For each observation of type Pain, the CPC shall be able to store the following data elements in addition to those listed in Section 6.3.2.1:
OBS- 54	• Pain Text Description (text) [E.g., “Lumbago”, “Neck pain”, “stomach cramps”]
OBS- 55	• Anatomic Location Text (text) [E.g., “Back”, “Left knee”, “Big toe”]
OBS- 56	• Anatomic Location Code (coded) [E.g., “94382793” {code= “Big toe”}]
OBS- 57	• Anatomic Location Coding System (coded) [E.g., “SNOMED”]
OBS- 58	• Severity Coding System (coded) [E.g., “1-10 scale”, “enumerated{mild,moderate,severe,worst ever}”]
OBS- 59	• Radiation? (coded) [Allowed values = “Yes” or “No”]
OBS- 60	• Pain Quality (text) [E.g., “Throbbing”, “Sharp”, “Aching”, etc.]
OBS- 61	• Onset (text) [E.g., “2 days ago”, “last week”]
OBS- 62	• Onset Timestamp Start Interval [E.g., “2007-11-09 00:00:00 GMT -0800”]
OBS- 63	• Onset Timestamp End Interval [E.g., “2007-11-09 23:59:59 GMT -0800”] (An interval is specified to formally represent varying granularity in the absolute time of onset, i.e., at some point during a specified hour, day, week, etc.)

OBS- 64	• Temporal Pattern (text) [E.g., “constant”, “intermittent”, “worst in the morning”]
OBS- 65	• Attempted Treatments and Effectiveness (text) [E.g., “Aspirin – didn’t help”, “rested – pain resolved”, “warm compress – a little relief”]
OBS- 66	• Perceived Precipitants (text) [E.g., “exercising”, “sitting at work”, “carrying baby”]

6.3.2.8. Type-Specific Attributes: Observable Parameter

This observation type is intended to record observations represented as “attribute/value” pairs, such as “heart rate : 75”, “blood glucose : 131”, or the gene loci evaluated by home DNA tests.

Note: This observation type is not intended to record presence or absence of discrete signs and symptoms, such as “fatigue”, “nausea”, “rash”, “palpitations”. The Sign or Symptom observation type is intended for such observations (see Section 6.3.2.6).

Table 6.10. Attributes of Observable Parameter Observations

Req ID	Requirement
	For each observation of type Observable Parameter, the CPC shall be able to store the following data elements in addition to those listed in Section 6.3.2.1:
OBS- 67	• Parameter Text (text) [E.g., “Blood Glucose”, “Range of Motion – Knee”]
OBS- 68	• Parameter ID (coded) [E.g., “10290293842” {code = “blood glucose”)]
OBS- 69	• Parameter ID Coding System (coded) [E.g., “SNOMED”, “LOINC”]
OBS- 70	• Value Type (coded) [E.g., “numeric”, “string”, “coded”] (Note: HL7 has a good list of value types for observations)
OBS- 71	• Value (<coding/format depends on Value Type>) [E.g., “130”, “50”, “9287928472” {code = “normal”}]
OBS- 72	• Value Units Text (text) [E.g., “mg/dl”, “%”,]
OBS- 73	• Value Units Code (text) [E.g., “MGPERDECI”, “PCT”,]
OBS- 74	• Value Units Coding System (code) [E.g., UCUM, ISO]

OBS- 75	• Recording Context - Text (text) [E.g., "Pedometer", "Depression scale survey APA-11 – Question 3", "Quality of Life Survey #6 – Question 22a"] (When relevant, this attribute records the means by which the observed parameter was collected. This may be particularly important when the responses to survey questions are recorded, because the responses may need to be interpreted in the context of the specific question asked.)
OBS- 76	• Recording Context - Code (coded) [E.g., "PEDMON" {code = "pedometer"}] (Note: These codes will be part of the common platform component data model; this attribute will not be used to record PHA-specific codes for recording contexts. PHA-specific codes may be recorded in the Additional Structured Data attribute.)

6.3.2.9. Type-Specific Attributes: General Observations

For observations documenting patient actions, events, and characteristics that are not addressed by the other observation types, a PHA may choose to store them as General Observations. In this case, the common observation attributes listed in Section 6.3.2.1 suffice to represent the data for these observations. Specifically, the attribute "Text Comment/Description" may be used to represent free-text data, and the attribute "Additional Structured Data" may be used to represent structured data.

6.3.3. Terminology Requirements for Observations

Due to the variety of observation types that the common platform component shall need to handle in a coded form, there are numerous requirements for the use of controlled terminologies in the CP:OBS component. The table below lists the concepts (in italics) that require a controlled terminology or coded data dictionary, as well as the coding system(s) (bulleted) that the CP:OBS component shall support for each concept. Note that the name of each concept is followed by the specific attribute(s) for which the coded concept shall be used. For example, a coded value for the concept *Medication* shall appear in the attribute *Medication ID* of the observation type *Medication Administration.*

Table 6.11. Requirements for Controlled Terminologies for Medication Management

Req ID	Requirement
OBS- 77	*Coded Medication* *[Medication Administration:Medication ID]*
OBS- 78	• The same code types as allowed for the "Identity of Medication" attribute in the CP:MED component
OBS- 79	• Proprietary drug coding systems (First Databank, Medispan, Multum)
OBS- 80	*Coded Physical Quantity Units* *[Medication Administration : Dose Amount Administered Units,* *Medication Administration : Physical Quantity Administered Units* *Meal/Snack : Meal Quantity Units,* *Meal/Snack : Ingredient Quantity Units]*
OBS- 81	• SNOMED
OBS- 82	• UCUM

OBS- 83	*Coded Medication Route of Administration* *[Medication Administration : Route of Administration]*
OBS- 84	• The same code types as allowed for the "Medication Intended Route" attribute in the CP:MED component
OBS- 85	• Routes in proprietary drug coding systems (First Databank, Medispan, Multum)
OBS- 86	*Coded Anatomy* *[Medication Administration : Site of Administration,* *Pain : Anatomic Location]*
OBS- 87	• SNOMED
OBS- 88	*Coded Physical Activity* *[Physical Activity : Activity ID]*
OBS- 89	• SNOMED
OBS- 90	*Coded Time Units* *[Physical Activity : Duration Units]*
OBS- 91	• SNOMED
OBS- 92	• UCUM
OBS- 93	*Coded Exercise Intensity Scale* *[Physical Activity : Intensity Units]*
OBS- 94	• Enumerated list of possible intensity scales, as defined in the CP:OBS component [e.g., "max HR achieved", "scale 1-10", "low,medium,high", "minutes before breaking a sweat"
OBS- 95	*Coded Meal Component* *[Meal/Snack : Food Item Code* *Meal/Snack : Ingredient Code]*
OBS- 96	• SNOMED
OBS- 97	*Coded Sign/Symptom* *[Sign or Symptom : Symptom Code]*
OBS- 98	• SNOMED
OBS- 99	*Coded Pain Severity* *[Pain : Severity]*
OBS- 100	• 1-10 scale
OBS- 101	• SNOMED
OBS- 102	*Coded Observable Parameter* *[Observable Parameter : Parameter ID]*
OBS- 103	• SNOMED

OBS- 104	*Coded Parameter Value Data Type* *[Observable Parameter : Value Type]*
OBS- 105	• HL7 Data Types for observations (e.g., “numeric”, “string”, “coded element”, “date”, “time”)
OBS- 106	*Coded Parameter Value* *[Observable Parameter : Value]*
OBS- 107	• SNOMED
OBS- 108	*Coded Parameter Recording Context* *[Observable Parameter : Recording Context]*
OBS- 109	• Enumerated list of possible contexts, as defined in the CP:OBS component

6.4. Required Functionality for the Observation Platform Component

Table 6.12. Required Functionality for the Observation Platform Component

Req ID	Requirement
OBS- 110	The component shall have the ability to *insert a new observation record* into the observation database for an existing patient when a PHA supplies all of the required attribute values and represents all attribute values using allowed formats and coding systems.
OBS- 111	The component shall have the ability to *modify an existing observation record* (as referenced by its Observation Unique ID) when a PHA represents all of the updated attribute values using allowed formats and coding systems.
OBS- 112	The component shall have the ability to *delete an existing observation record* (as referenced by its Observation Unique ID)
OBS- 113	The component shall make all modifications to and deletions of existing observations records “non-destructively,” i.e., a record of the previous values of any modified or deleted observation records will be retained within the system, along with a record of when the modification/deletion occurred and which user requested it (see Audit Logging in Section 7.5).
OBS- 114	The component shall have the ability to retrieve and return to a PHA all attributes of all the observation records for a specified patient in a single operation
	The component shall have the ability to return to a PHA a subset of the observation records for a specified patient based on a query expression that includes type-appropriate comparisons (>, <, =, LIKE, IS-A) and Boolean combinations (AND, OR, NOT) involving the following attributes:
OBS- 115	• Observation Unique ID
OBS- 116	• Observation Type
OBS- 117	• Observation Sub-Type

OBS- 118	• Observation Coded Identifier [Note: The type of identifier tested will depend on the observation type; see the mapping table below: Observation Type — Attribute Name Medication Administration — Medication ID Physical Activity — Activity ID Sign or Symptom — Symptom Code Observable Parameter — Parameter ID (Certain observation types may not include a coded identifier.)
OBS- 119	• Text Comment/Description
OBS- 120	• Observation Entry Datetime
OBS- 121	• Observation Effective Start Datetime
OBS- 122	• Observation Effective End Datetime
OBS- 123	• Reference/Link to medication-list record (Medication Administration records only) [Note: Selection by this attributes allows a PHA, for example, to retrieve all of the medication administration observations related to a specific medication on the med list.]
OBS- 124	For query expressions that involve one of the *Observation Coded Identifiers*, the component shall be able to perform "IS-A" comparisons between the query parameters and the observation data. For example, a query expression may contain the logic "return all observations of type Sign or Symptom where the Observation Coded Identifier IS-A respiratory-symptom."
OBS- 125	The CPC shall have the ability to return to a PHA a specified *subset* of the common attributes of the observation record(s) for a specified patient. The specified subset may include any combination of the available common attributes.
OBS-125.1	The component shall allow a PHA to *subscribe to observation records* for specific patients, such that whenever an observation of a particular type (or of any type) is inserted or updated, the component shall automatically notify the PHA and transmit the corresponding observation data to the PHA.

Requirements Questions

Req ID or Section	Question
	N/A

7. Identity Management

The ability to authenticate the users of a PHA and to determine the access privileges that a user account has with regards to a given health record are requirements of a number of PHA projects. In certain cases, the identity management component requirements came from the descriptions of functionality that the PHAs plan to support. In other cases, requirements were derived from an understanding of the HIPAA regulations for privacy and security of patient health data.

The requirements in this section are focused on describing the functionality of the Identity Management System (IMS) Common Platform Components. For the purposes of the Project HealthDesign, Identity Management consists of four key functions:

(1) Registration and identity-validation of users

(2) Authentication of user upon login

(3) Access Control (a.k.a. Authorization)

(4) Audit Logging

This section describes the requirements for these key topic areas and how they fit together to specify the Common Platform Component *Identity Management System* (CP:IMS).

7.1. PHAs and Identity Management

A first step in defining the functional requirements of the Identity Management components is to enumerate the functions that PHAs using the platform may need to protect patient health record information. Table 7.1 lists these requirements as elicited from the nine grantees of Project HealthDesign.

Table 7.1. PHA functions that require Identity Management

No.	Function
1	Provide a secure environment for patient data so as to ensure that patient data is protected from unauthorized access.
2	Allow patients to control who may view data in their personal health record.
3	Allow patients to control who may add or change data in their personal health record.
4	Allow patients to control what kinds of data are accessible to other users.
5	Allow patients to control which applications may use their data on behalf of the patient
6	Allow patients to logically group other users and assign roles (i.e., a patient's physicians and family members) with respect to their health record to simplify administration of access control
7	Allow patients to review an accounting of all access to their personal health record.

7.1.1. Identity Management Models and Dataflow

There are two general cases to consider when discussing the Identity Management component requirements. In the first case, a stand-alone PHA is connected to a single instance of the CP:IMS. Here, stored data and users are exclusive to the single PHA. This case will be referred to as the "**Stove-Pipe**" model and a diagram of this configuration is shown in Figure 7.1. The figure shows the conceived CP:IMS functioning as a User Authentication service, a User Registry, and an Access Control service for the PHA.

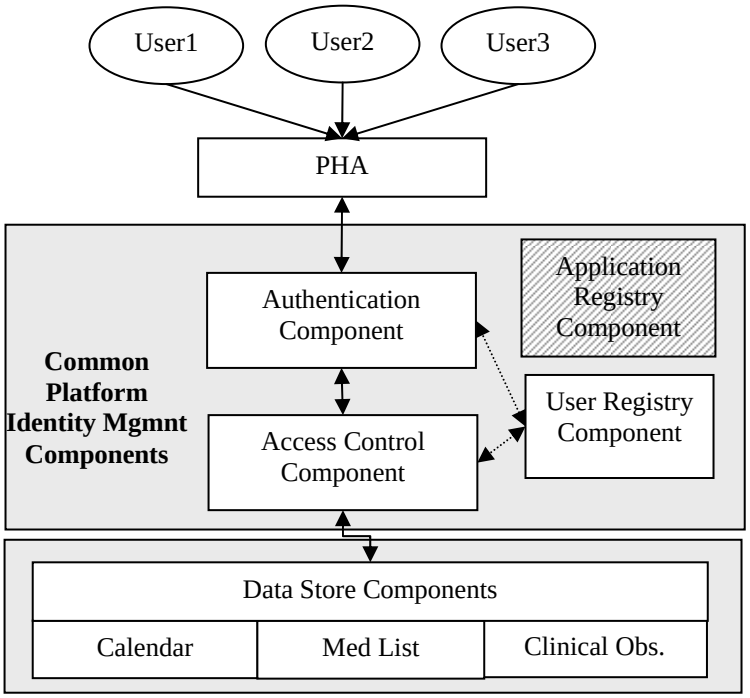

Figure 7.1 Common Platform Component Architecture: Stove-Pipe Model

In the second case, we consider a CPC architecture to which multiple PHAs are connected. With this hub-like architecture, data stored in the data store components may originate from or be provided to any of the connected PHAs and a user may utilize one, multiple, or all of the PHAs connected to the CP:IMS. This case will be referred to as the "**Hub**" model and a diagram of this configuration is shown in Figure 7.2

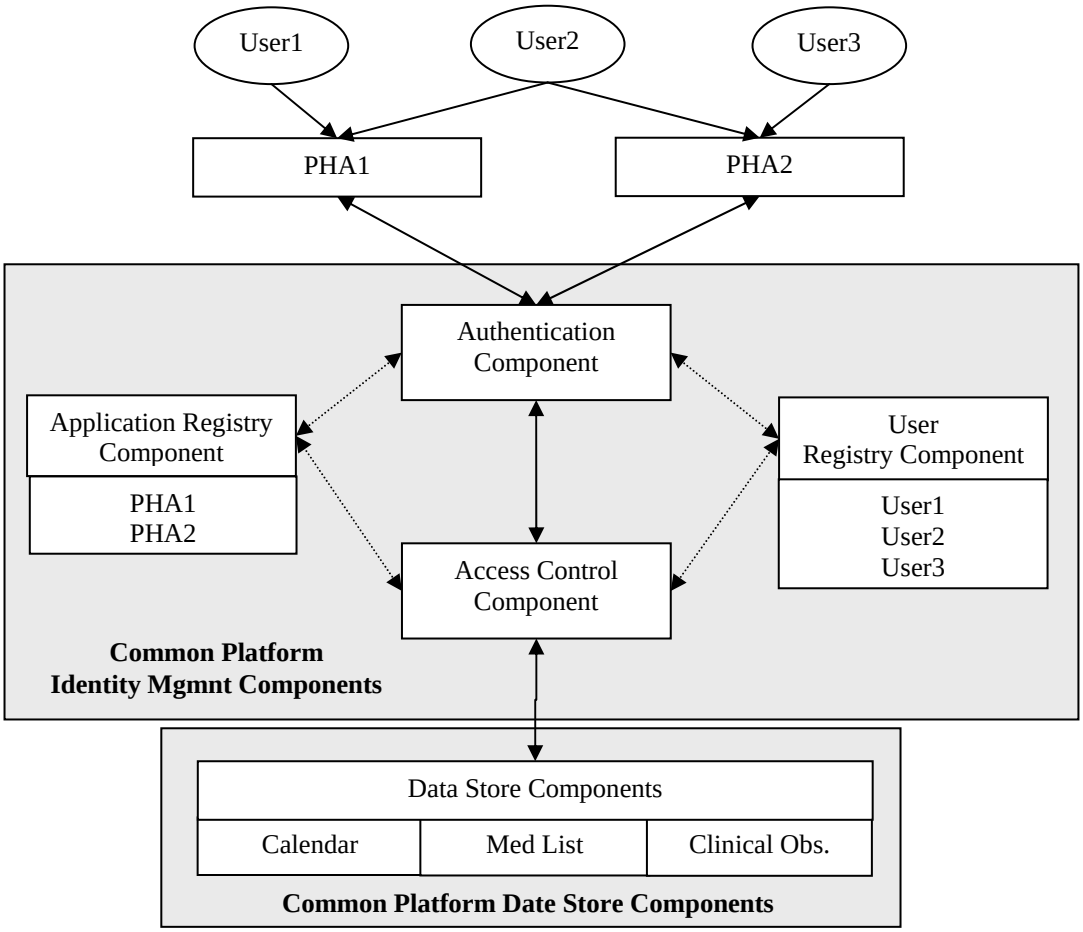

Figure 7.2 Common Platform Component Architecture: Hub Model

The requirements of the CP:IMS address both of the above cases. For certain requirements, special considerations are described that support one particular model or the other. However, care has been taken to identify requirements for these two architectures in as unified a manner as possible.

A general requirement of the Common Platform Components is to allow PHAs to use each component separately or together as a single unified solution. For example, a PHA should be allowed to use the Authentication and User Registry components to serve as the authentication and user registration solutions for the PHA without using any of other components of the platform. Figure 7.3 shows a system diagram of such a configuration (note that the Application Registry and Access Control Module are not being used in this configuration of the components).

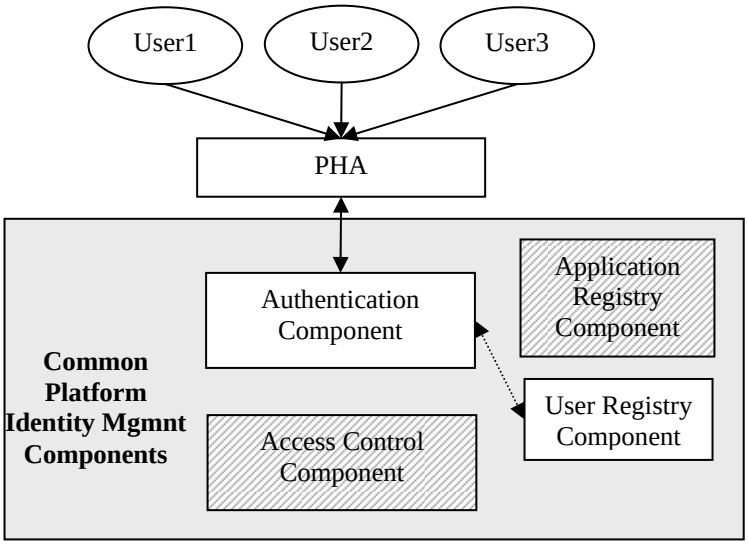

Figure 7.3 Identity Management System: User Registry & Authorization Components Only

7.1.2. Authentication and Access Control: Dataflow

Below is a proposed dataflow that describes the **authentication**, **user registry interaction**, **access control**, and **data access** actions that take place during the course of a user's interaction with a PHA connected to any instance of a common platform component. The intent of the dataflow diagram is to put the requirements for the CP:IMS described in this section into context for the reader, not to indicate any specific design requirements for an implementation of a PHA or a common platform infrastructure. The steps described in the process workflow description refer to the numbered areas of Figure 7.4.

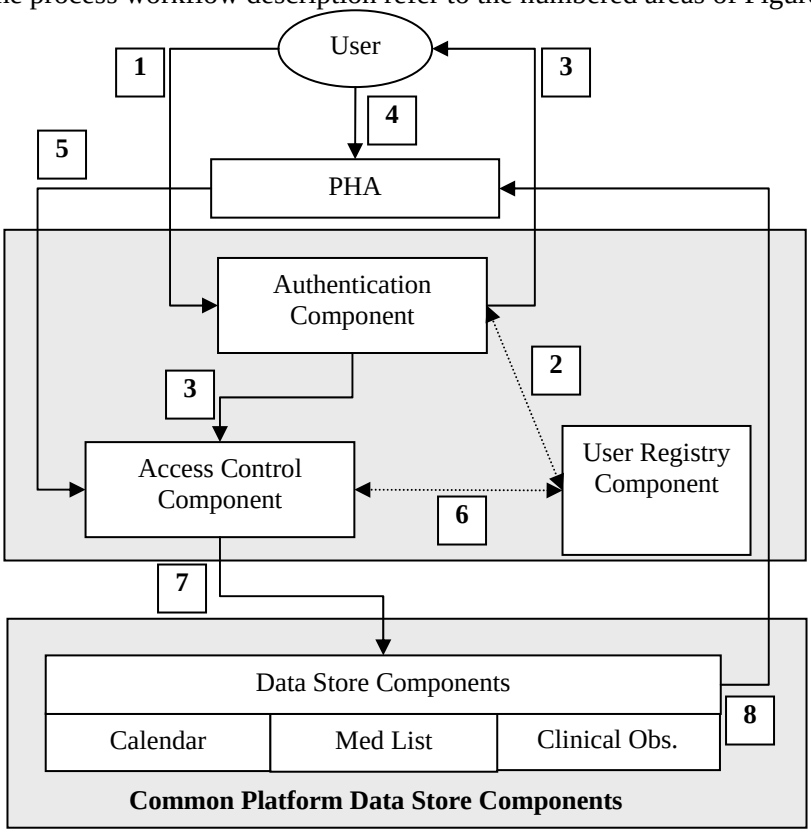

Figure 7.4 Authentication and Access Control Dataflow Diagram

(1) The user provides login credentials to the authentication component.

(2) The authentication component checks the user's login credentials against the credential information stored in the user registry component.

(3) Upon successful confirmation of the user's login credentials, the Authentication component generates an authentication token for the user session and sends that token back to the user as well as registering it with the Access Control component.

(4) The user makes a request for patient data stored in the Data Store components through a PHA connected to the platform.

(5) The PHA uses the authentication token from the user and passes the data request and authentication token to the Access Control component.

(6) The Access Control component checks the authentication token that is received in the request against the registered authentication token, and determines whether the requesting user has been properly authenticated. If so, the Access Control component passes the data request to the Data Store Components.

(7) The Data Store components generate a response that contains the personal health data that (1) the user requested and (2) the user has access to (possibly a subset of the data requested). The components return that response to the originating PHA.

7.2. Required Functionality for a User & Application Registry Platform Component

Table 7.2 describes the requirements around identifying data providers, data consumers, and various applications that will interact with resources of the Common Platform. In addition, requirements surrounding the registration of users with the CP:IMS are described.

Table 7.2. Requirements for Registration/Identification Common Platform Component

Req ID	Requirement
IM- 1	The CP:IMS shall require any user or business entity with access to resources in the CP to be uniquely identified within the user registry component. The term "user" may include the patient (record owner), a physician, a family member, caregivers, or any other individual who utilize a PHA to view/edit personal health data on their own behalf or on behalf of another individual (patient). The term "business entity" may include organizations such as health plans covering the patient, e-prescribing networks that transmit prescription data on behalf of a patient, or many other health-focused organization that may act as a data provider/consumer
IM- 2	Any PHA that interacts with the CPC resources shall be uniquely identified (e.g., the application has been assigned a unique application id) within the application registry component. PHAs without a valid application id shall not be granted access to CPC resources.
IM- 3	External applications and PHAs that must connect to the Data Store components in order to provide or consume data shall be assigned a user id just as any system user would. The user id shall be a proxy for the common platform client application and will enable the access control system to execute decision logic to determine how the application may access patient records. An example of an external CPC client application is an interface engine that takes HL7 messages from a laboratory feed and updates a patient's personal health record with laboratory data.

IM- 4	Identities of data providers/consumers/applications that interact with the data present in the Common Repository shall be verified (via an identity assertion/certification mechanism) to ensure that the person requesting access to the common platform is in fact who they claim to be.
IM- 5	Each user/application account maintained within the Identity Management System shall contain the information necessary to adequately identify the user/application including demographic information, message routing information, and identity certification (i.e., proof that the user account was verified as described in requirement IM- 4).
IM- 6	The common platform shall make available to PHAs information about registered users/applications (including the identifying information and identity certification necessary to validate the identity of a data provider/consumer). This requirement will allow a record subject to locate an account holder or external application with which to grant access to the personal health record.
IM- 7	PHAs shall be allowed to use the user/application registry component as a stand-alone component without using or implementing any other components of the CP:IMS (i.e., the authentication and access-control components). This requirement supports the general requirement for the CP to provide component solutions, in addition to a unified solution. The user registry component shall be usable as part of a PHA "stove-pipe" application to fulfill the specific PHA requirements for the storage and retrieval of user account information.
IM- 8	In the case that the CP:IMS is implemented as a "hub" model, the user registry component shall be the exclusive user registry system utilized by any PHA that connects to the CP to request services. This requirement addresses the need to have consistent user authentication and identification to fully support the requirements for access control in a distributed system.
IM- 9	The user/application registry component shall provide a means to allow new users to register and provide all necessary identification information (including identity certification). Once a user has been registered and their identity has been verified (per requirement IM- 4), that user may begin to store and retrieve information via any PHA connected to the CP on which the user is registered.
IM- 10	The user/application registry component shall provide a means to allow registered account holders to manage the account information stored in the component. This includes the update and deletion of information stored in the account. Specific kinds of account information shall include but is not be limited to Name, Gender, Date of Birth, Address, and contact information (phone, email, SMS#, IM account, etc.)

7.3. Required Functionality for an Authentication Platform Component

Table 7.3 describes the requirements around authentication between PHAs and the authentication component of the CPC. It is assumed that, in most cases, the PHAs that connect to the CPC will use the services of the authentication component as the application's exclusive authentication system. However, this may not always be the case and a PHA may utilize a separate authentication system to grant access to the PHA. If the CPCs are implemented in the "Hub" model, allowing any number of PHAs to connect to shared resources of the CP, the CPC shall enforce that users authenticate with the authentication component separately from any authentication required by individual PHAs. This general requirement is necessary to guarantee the security of the data in the shared environment.

In addition to requiring users that connect to the CPCs to be authenticated, the PHAs themselves must provide authentication credentials to prove to the authentication component that the request for data is coming from a trusted source. Conversely, to guarantee the security of data that is returned to PHAs from the CPCs, the authentication component will provide a set of authentication credentials to PHAs connected to the CPCs.

Table 7.3. Requirements for Authentication Common Platform Component

Req ID	Requirement
IM- 11	PHAs shall be allowed to use the authentication component as a stand-alone component without using or implementing any other component of the CP:IMS (i.e., the user/application registry component or the access control component). This requirement supports the general requirement for the CP to provide component solutions, in addition to a unified solution.
IM- 12	The authentication component shall be configurable so that it may be "pointed at" any user/application registry system including the CP:IMS registry component or an externally developed registry system.
IM- 13	In the case that the CP is implemented as a "hub" model, PHAs that connect to the CP shall provide an authentication token generated by the CP:IMS authentication component in order to grant users access to data resources stored in the CP. This does not preclude PHAs from implementing other forms of authentication but does require the PHA to support the CP authentication protocols in addition to any other authentication scheme specific to the PHA. This requirement addresses the need to have consistent and trusted user authentication in a shared environment.
IM- 14	The CP:IMS authentication component shall support direct user authentication using password, two-factor identification, or biometric reading schemes.
IM- 15	The CP:IMS authentication component shall generate an authentication token for users upon successful authentication. PHAs shall use these generated tokens to confirm the authentication status of the user account requesting resources within the CP during subsequent requests for CP resources. Authentication tokens shall have a finite lifetime (duration TBD).
IM- 16	PHAs that connect to the CP:IMS shall provide valid application specific authentication credentials (e.g. an application id and an application specific password) to verify that the PHA has authorization to connect to the CP. The authentication of these credentials shall allow a PHA to establish a connection to the CP and access publicly available data (e.g. a generic medication list, data dictionary information, etc).
IM- 17	In addition to requiring application specific credentials (app id & app password) to allow PHAs to connect to the CP resources, the authentication component shall require PHAs to also provide a user account id and password specific to the PHA. These "user" account credentials will allow access control logic to be applied to PHAs that must access patient record data outside the context of an explicit user session.
IM- 18	The CP:IMS shall authenticate itself to the PHA in all responses from the CP to the PHA (e.g., verified certificate, session id, app id/password etc.). This shall allow PHAs connected to the CP to confirm that the origin of the response came from the CP as expected and is legitimate.

7.4. Required Functionality for an Access Control Platform Component

Access Control (AC) is the cornerstone of the IMS. The requirement to allow the record owner to control access to the patient's personal health record information with regards to other individuals is a very common requirement among the Project HealthDesign participants. To meet this general requirement, an access control component is needed that manages Common Platform resource access. This module shall base access decision logic on five distinct dimensions

(1) **Record** – the health record being accessed

(2) **Actor** – the user with a specific role (with respect to a specific patient record) seeking access (see explanation below);

(3) **Action** – the specific type of access being sought;

(4) **Resource** – the data element(s) to be accessed;

(5) **Environment** – the PHA being used to access the resource.

Before describing the requirements of the access control system, it is necessary to clearly distinguish between the concepts of a "User Account" and a "Health Record".

User Account: refers to a person's ability to access the common platform and is composed of the user's credentials used for authentication purposes as well as certain demographic data used to identify a user of the CPC. A User Account may have access to zero or more Health Records. Patients, parents of patients, physicians, and others may have a User Account. Specifically, having a User Account does not require that the user have any personal health data stored in the system.

Health Record: refers to a patient's personal health information. It includes a patient's medication list, calendar, observations, and any other health related information stored by the CPCs. A Health record has exactly one Record Subject (the person to whom the heath record relates). Access to a health record may be shared with one (the Record Subject) to many User Accounts. In some cases, the Record Subject may not control their own Health record (such as when a parent controls the record of a child). In these cases, the parent is referred to as the Record Custodian.

The general requirement for access control in the CPC is to allow Record Subjects and Record Custodians to control access to their personal health records. Health Record access may be granted to a specific User Account or to any User Account that has been assigned a particular *Role* with regards to a specific Health Record. The role of a specific user account shall be assigned by the Record Subject or Record Custodian within the context of the patient's Health Record. This association between User Account Id, Health Record Id, and the type of *Role* will be stored by the access control component and used to apply access control rules to the User Accounts assigned to a particular group by the Record Subject/Custodian.

Allowing Record Subjects to grant access at the level of a *Role* simplifies the administration of access rules for individuals by providing the ability to apply rules across an entire logical group of users. For example, if a user wishes to change the access control rules for a logical group of accounts (i.e., all of the patient's physicians), the Record Subject is required only to change the rule once at the level of the *Role* to have it applied to every account assigned to that group.

Below are some examples of access control rules based on the requirements gathered from project leaders. Following each access control rule description is a table that lists the five dimensions of the access control component that determine the access rule. In some cases, multiple entries are required to fully describe an access rule. Examples of these types of access control rules might include:

1. Allow my doctors to view all information (including annotations and record history) in my personal health record. My doctors may have this access using any approved PHA.

Rule	Rec.	Actor	Action	Resource	Environment
101	123	Physician	Record Viewing	All Health Records	All Apps

2. Allow my doctor (user id: dr_wolf@cpc.org) to view only my medication list. My doctor may make annotations to the medications but may not add or edit medications.

Rule	Rec.	Actor	Action	Resource	Environment
202	234	dr_wolf@cpc.org	Record Viewing	Medications	All Apps
202	234	dr_wolf@cpc.org	Annotate Record	Medications	All Apps

3. Allow my entire family to see my entire medication list (not including annotations or history), but do not let them see any medications that are anti-depressants or bipolar agents.

Rule	Rec.	Actor	Action	Resource	Environment
303	345	Family	Read Record	Medications	All Apps
303	345	Family	Protect Record	Anti-Depressants	All Apps
303	345	Family	Protect Record	Antipsychotics	All Apps

4. Allow my case managers to see my food blog, latest blood glucose readings, diabetic medications, and exercise events on my calendar.

Rule	Rec.	Actor	Action	Resource	Environment
404	456	Case Manager	Read Record	Blog	All Apps
404	456	Case Manager	Read Record	Blood Glucose Reading	All Apps
404	456	Case Manager	Read Record	Diabetic Agents and Monitoring	All Apps
404	456	Case Manager	Read Record	Exercise Events	All Apps

5. Allow my children to administer my personal health record including the ability to grant read/write access to my account to others. Do not allow my child to grant administrative rights to others.

Rule	Rec.	Actor	Action	Resource	Environment
505	567	Child	Grant Record Modification Privileges	All Health Records	All Apps
505	567	Child	Grant Record View Privileges	All Health Records	All Apps

6. Allow Quest Diagnostics (user id: questlabloader@cpc.org) to post lab results to my medical record but only using the "QuestLabLoader" application (application id: 12345)

Rule	Rec.	Actor	Action	Resource	Environment
606	678	questlabloader@cpc.org	Insert Record	Lab Data	12345

Table 7.4 lists the specific functions and operations that the access control component shall be able to perform.

Table 7.4. Requirements for the Access Control Common Platform Component

Req ID	Requirement
IM- 19	The access control component shall compare information provided in the request including the user making the request (actor), the application being used to make the request (environment), the resource being requested (resource), and the type of action being performed (action) against a defined set of rules. The access control component shall enable data and data operation requests/responses to be filtered so as to ensure that user accounts that request data access have adequate authorization to do so. This would include viewing data as well as performing modifications to the data (insert, update, delete, etc).
IM- 20	The access control component shall provide a set of default access control rules that are assigned to a patient record upon creation.
IM- 21	Each record shall have an independent set of access control rules that may be customized to fit the access control preferences of that specific record.
IM- 22	Record Subjects shall be able to view rules that have been created and associated with their record.
IM- 23	Patients shall be able to create new access control rules for their record.
IM- 24	Patients shall be able to edit existing rules for their record.
IM- 25	Patients shall be able to revoke any access rules that exist for their record at any time for any reason. This includes a PHA's access to data resources that may be necessary for the PHA to perform certain functions with the patient's record.
IM- 26	The access control system shall never restrict the access of a Record Subject to the record itself. Record Subjects shall never be able to "lock themselves out" of any part of their own record, nor be locked out by a record custodian.
IM- 27	The CP shall allow a Record Subject and a Record Custodian to assign a Role to another user account within the context of a record.
IM- 28	A user account shall have 0 or more Roles assigned with regards to a specific record. This requirement removes the need for record subjects/custodians to make arbitrary judgments on what role to assign to another account. For example, a record subject assigns the role of "Child" to her daughter, who happens to also be the record subject's doctor, and so the daughter is also assigned the role of "Doctor" on the mother's account. This allows the grantee to see data that the record subject's other doctors could see (and possibly data that "Children" could not see) but would allow the grantee to also see data that the subject's children could see (and possibly data that "Doctors" could not see).
IM- 29	In the event that a user has multiple roles assigned with respect to a single record, the access control service shall grant the most permissive access based on the defined role rules.
IM- 30	A user account shall be allowed to have different roles assigned for different records. For example, Dr. John Doe may be identified as the "Record Subject" role for Record1, a "Child" role for Record2, and a "Doctor" role for Records 3, 4, and 5.
IM- 31	The access control component shall maintain a registry of the role relationships established between user accounts and records.

IM- 32	The access control component shall provide a list of user roles to PHAs that correspond to the user roles understood by the access control system. This will allow PHAs to discover and display the list of defined account roles that a Record Subject may assign to another account (and are understood by the access control module for the purposes of limiting access).
IM- 33	PHAs shall be allowed to use the access control component without using any other component of the CP:IMS (i.e., the registration and authentication components). This requirement supports the general requirement for the CP to provide component-based solutions, in addition to a unified solution.
IM- 34	The access control component shall be configurable so that it may be "pointed at" any user registry system, application registry system, or a persistent data store including the implementations of the CP:IMS components or any external implementations of these components.
IM- 35	The hierarchical ontology (see Section 7.4.1 below) and the mapping of the ontology to a data store shall be extensible, allowing new concepts and concept categories to be added and existing concepts to be modified. This requirement supports the use of the access control component with an external data store (see requirement IM- 33) that may have a data model that differs from the data model supported by the CP.
IM-35.1	The access-control component shall be able to constrain a user's access to a specific record to only that time during which another user is logged into the record (i.e., the time during which a valid authentication token exists for that other user). This feature will allow, for example, record subjects to share their records only while they, themselves, are logged in and able to monitor who is accessing their record
IM-35.2	The access-control component shall be able to *temporally* constrain a user's access to a specific record to only a specified window in time (i.e., as delineated by a start and stop date/time). This feature will allow, for example, a caregiver to share a medical record only while he is on vacation or only for the next 24 hours.
IM-35.3	The access-control component shall be able to constrain a user's access to a specific record to only a single login (i.e., the time during which only the first authentication token that the user is granted is valid – access to the record will not be granted during any subsequent logins, although the user may potentially be able to access other records during subsequent logins).

7.4.1. Ontological Hierarchies of the Access Control Component

To support the generation of the access control rules, we have developed and proposed a simple hierarchical ontology to represent the possible categories of concepts that can be specified in the Actor, Action, Resource, and Environment dimensions of the access control rules. The intended goal of these hierarchies is to allow users to have the flexibility to set permissions at a very high level of granularity (e.g., a rule that applies to "Health Care Providers"), at a medium level of granularity (e.g., a rule that applies to "Doctors", any doctor identified as having access to a particular record), or at a very low level of granularity (e.g., a rule that applies to a specific doctor account, "dr_wolf@cpc.org", just one of a patient's identified doctors).

Access controls rules shall be applied in a hierarchical fashion, with lower-level concepts in the Actor, Action, Resource, and Environment hierarchies inheriting the access-control privileges of higher level concepts (unless otherwise over-ridden). For example, if no access-control rules have been defined specifically for "pharmacists", then pharmacists will inherit the access control rules defined for "Health Care Providers). Similarly, all individual users with the role of "Family Member" will be granted the

access privileges associated with that role, except for those individuals who have been explicitly denied certain privileges.

The following tables contain the categories that we have determined are pertinent to access control of a personal health record. It is important to note that (unless otherwise indicated) the final "leaf" at the end of each hierarchical tree node is at the level of an individual instance of a "concept" (e.g. a specific user account or medication) although it may not be explicitly displayed (for simplicity of documentation).

Table 7.5 displays the hierarchy of roles that a record subject or record custodian may assign to another's user account in relation to a specific health record so as to define the person's relationship to the record subject.

Table 7.5. Actor Hierarchy (Roles)

Req ID	Role	Comment
~~IM- 36~~	~~All Users~~ Requirement deleted. See req. IM-38.1	~~The root account type. All account types have user as the base type.~~
IM- 37	Record Subject	This is the user to whom the personal health record refers.
IM- 38	Record Custodian	Any user who is not the account subject that may control the record on behalf of the account subject (e.g., a parent that controls a child's record or a home care giver that controls an elderly patient's record)
IM- 38.1	All Other Users	The root account type for all users who are not the Record Subject or the Record Custodian.
IM- 39	Family Member	
IM- 40	Parent	
IM- 40.1	*Account Instance*	A specific user account
IM- 41	Child	
IM-41.1	Sibling	
IM- 42	Health Care Provider	An individual user that works in the medical field and provides care for the account subject.
IM- 43	Physician	
IM- 44	Registered Nurse	
IM- 45	Physician Assistant	
IM- 46	Clerical Personnel/ Office Staff	
IM- 47	Home Care Provider	

IM- 48	EMT	
IM- 49	Pharmacist	
IM- 50	Nutritionist	
IM- 51	Personal Trainer	
IM- 52	Physical Therapist	
IM- 53	External Application	External applications that need read or write access to resources in the CP must be registered as users. This category is the parent for any type of external application
IM- 54	HIS System	
IM- 55	ADT System	
IM- 56	EHR System (Ambulatory)	
IM- 57	Practice Management System	
IM- 58	RHIO	
IM- 59	Health Plan	
IM- 60	e-Prescribing Network	
IM- 61	Laboratory System	
IM- 61.1	*Specific External App*	

The actions described in Table 7.6 represent the kinds of operations that may be performed via the API to the CPC. Instance level record identification is not applicable to the actions described in the action hierarchy (i.e., there is no implicit *Instance* level leaf in this tree).

Table 7.6. Action Hierarchy (Type of Record Access)

Req ID	Action	Comment
IM- 62	All Operations	The root action type. This level of access should only be granted to the record owner in most cases
IM- 63	Record Modification	Access granted at this level allows full write/update/delete control over allowed health data resources. Data is still restricted along the resource type dimension.
IM- 64	Insert Record	

IM- 65	Annotate Record	Add a comment to an observation without changing the observation itself.
IM- 66	Update Record	Non-destructive
IM- 67	Delete Record	Non-destructive
IM- 68	Mask Record	Make record existence notable to other users but keep the details obscured
IM- 69	Record Viewing	Access granted at this level allows view record viewing rights for an allowed resource.
IM- 70	Read Record	
IM- 71	Read Annotation	
IM- 72	Read Record History	Because changes to data in the CP are never destructive, a history of all changes to a resource is maintained. Access to this privilege allows a user to view the full history of changes to data.
IM- 73	Record Administration	Access granted at this level gives users the ability to set resource access privileges and delegate that right to others.
IM- 74	Record Protection	Includes preventing a certain user role from accessing a certain kind of resource at a fine grain when access has been granted to a broader category (e.g., preventing a family member that has been granted the privilege to see a patient's full med list from seeing the patient's anti-depressants and anti-psychotics)
IM- 75	Grant/Revoke Record Modification Privileges	Users with this access may grant the right to modify CP resources to other users
IM- 76	Grant/Revoke Record Viewing Privileges	Users with this access may grant the right to view CP resources to other users
IM- 77	Grant/Revoke Record Administration Privileges	Users with this access may grant the right to administer a health record (i.e., grant/revoke rights) to other users

The ontology shown in Table 7.7 represents the kinds of records that may be controlled by the Access Control CPC.

Table 7.7. Resource Hierarchy

Req ID	Resource	Comment
IM- 78	All Health Data	The root data resource type. Access granted at this level would include every kind of data in the CP Data Store.
IM- 79	All Medication List Items	The entire medication list for a record
IM- 80	<Medication Category>	Examples of medication category include Cancer Therapy Agents, Central Nervous System Agents, Cystic Fibrosis Agents, Diabetic Agents, Over-the-Counter Medications, etc.
IM- 81	<Medication Sub-Category>	Examples of medication sub-category include Analgesics, Anti-depressants, Mucolytics, Contraceptives, Oral Anti-diabetic Agents, etc.
IM- 82	<Generic Medication Name>	
IM-82.1	*Medication Instance*	A particular instance of a medication in a medication list
IM- 83	All Calendar Entries	The entire calendar(s) of events for a record
	All Calendar Events	
IM- 84	~~Calendars~~ *Original Requirement Deleted* – Separate calendars were not addressed in body of requirements	~~Control access to information on separate calendars independently.~~
IM-84.1	Medical Events	
IM- 85	Medication Administration	
IM- 86	*Event Instance*	A particular instance of an event
IM- 87	Medical Appointment	
IM- 88	~~Outpatient Appts~~	
IM- 89	~~Inpatient Appts~~	
IM- 90	~~Rx Refills~~	
IM-90.1	Observation Recording	
IM- 91	Personal Events	
IM- 92	Physical Exercise	
IM- 93	Sleep	
IM- 94	Meal/Snack	
IM-94.1	School/Work	
IM- 95	~~Deadline~~ *Original Requirement Deleted* -- now handled by Calendar Tasks	
IM-95.1	All Calendar Tasks	
IM-95.2	Medical Tasks	
IM-95.3	Medication Refill	
IM-95.4	Medical Appointment	
IM-95.5	Observation Recording	

IM-95.6	Personal Tasks	
IM-95.7	Physical Exercise	
IM-95.8	Sleep	
IM-95.9	Meal/Snack	
IM-95.10	School/Work	
IM- 96	All Observations	All observations in daily living collected for a record
IM- 97	All Personal Observations	All observations that are recorded by the record subject (or on behalf of the record subject via a device interface)
IM- 98	Medication Administration	
IM-98.1	*Observation Instance*	A particular instance of a medication administration observation.
IM- 99	Sign or Symptom	E.g., irregular heart beat, shortness of breath
IM- 100	~~Mood~~	
IM- 101	Observable Parameter	E.g., Weight, mood, bl. glucose
IM- 102	~~Weight~~	
IM- 103	~~Blood Glucose~~	
IM- 104	~~Blood Pressure~~	
IM- 105	Pain	
IM- 106	Meals/Snack	
IM- 107	~~Composition~~	
IM- 108	~~Photos~~	
IM- 109	Physical Activity	
IM- 110	~~Survey Information~~	
IM- 111	Journal Entry	
IM-111.1	General Observation	
IM- 112	All Audit Records	

The simple hierarchy listed in Table 7.8 describes how applications that may be categorized to grant access to a specific health record.

Table 7.8. Environment Hierarchy

Req ID	Resource	Comment
IM- 113	All Applications	The root environment type. Access granted at this level would include every application registered with the CP:IMS
IM- 114	*Application Instance*	A specific instance of an application connected to the CPC

7.5. Required Functionality for an Auditing Platform Component

Table 7.9 describes the requirements around auditing access to a patient's health record.

Table 7.9. Requirements for Auditing Common Platform Component

Req ID	Requirement
IM- 115	The auditing component shall maintain an audit log of every user and application insert, update, and data retrieval from the CP.
IM- 116	The auditing component shall contain the following information for each and every operation: • User Account id • Application id • Record id (i.e., the ID of the entire medical record) • Resource requested (the ID of the specific event, observation, etc. record) • Action (e.g., view, insert, update, annotate, etc.) • The request outcome (authorized, rejected, etc.) • System Timestamp of the request • The IP address from which the request originated
IM- 117	The timestamp recorded in conjunction with each audit log component entry shall be corrected to GMT and stored as such. For example if an Record Subject views her medication list at 9:00 p.m. EDT on November 1, 2007 then the timestamp recorded in the audit log would be "2007-11-02 01:00:00 GMT -08:00". The time zone of the originating system shall be recorded to back-calculate the time of the log entry.
IM- 118	Record subjects shall have read access to audit log events that pertain to their record id.

Requirements Questions

Req ID or Section	Question
IM- 16	Q: Can we forego application specific authentication when the CP is implemented as a "Stove-Pipe" model? A: No, it should still be built into the model, although a universal, non-expiring authentication token could be built into stove-pipe applications, such that requests from the PHA to the stove-piped platform component would also be serviced (i.e., it will be assumed that the PHA will not make any requests unless it has first authenticated the user).
	Q: Is it a requirement to allow users to control access to calendar events based on the time of the event? E.g., only show others events that occur during the week-day. A: No.

8. Glossary

Term	Definition
Access Control	The mechanism and process of controlling which users have access to which resources in a personal health record. Access controls determine whose records a user may access, what kinds of data in those records a user may access (e.g., medication data, calendar data, etc.), and what operations a user may perform on those data (e.g., read-only, insert-only, modify, etc).
Annotation	Additional information added to specific data in a Personal Health Record to provide commentary or explanation. Annotations are often added by someone other than the user who added the original data, as permitted by the relevant access controls.
Audit Logging	The process of recording ("logging") detailed information about data-entry events and data-access events related to a specific Personal Health Record for the purpose of later verifying that only legitimate and authorized access took place. Audit logging typically entails recording the identity of the user who requested access, the time of the access, the operation(s) performed during the access, and any relevant information about the purpose of the access.
Authentication	The process of verifying that a person or process attempting to log into a personal health application under a specific user account is, in fact, the user that the person or process claims to be. Authentication typically involves submission and verification of a password or other information specific to the user account (such as a biometric pattern or transient SecurID parameter).
Authentication Token	In general, a hardware or software device that, when in the possession of a person or process, enables the person/process to be authenticated as a registered user of a computer application. Examples include smart cards (hardware) or digital certificates (software). In the specific case of the Identity Management component described in Section 7.3 of this document, the authentication token is an encrypted software token that verifies that the user was successfully authenticated by the Authentication Platform Component. The token is subsequently used by the Personal Health Application and various common platform components to grant access to the user.
Calendar Event	An event, appointment, or task that appears on a calendar and that is scheduled to be performed at a specific time or over a specific time interval. For example, a medical appointment, a meeting, a scheduled drug administration.
Calendar Reminder	An instruction associated with a Calendar Event or Calendar Task to inform the user at a specified time about the event or task. Calendar Reminders may be sent to various users through various media, as specified in the reminder.
Calendar Task	A task or goal that is intended to be performed or achieved and that may be associated with a deadline recorded on a calendar. Distinct from Calendar Events in that Calendar Tasks are not scheduled or intended to be performed at a specific, pre-determined time.
Dosage Form	The physical medium by which a medication is administered. For example "tablet", "capsule", "syrup", "transdermal patch", "solution for injection"
Dosing Frequency	The timing with which a medication should be taken. For example "once per day", "every 6 hours", "before bedtime", "as needed"
EHR	See "Electronic Health Record"

Electronic Health Record	A computerized medical record maintained by a health care organization or health care provider. Distinct from a Personal Health Record in that the health care organization or provider typically controls the contents of and access to an EHR, whereas the patient typically controls the contents of and access to the PHR.
Generic Ingredient	The chemical ingredient(s) of a medication (usually an active ingredient). For example, "Ibuprofen". The generic ingredients define the therapeutic effects of the medication. Multiple brand names may correspond to the same generic ingredient (e.g., "Advil", "Motrin", "Wal-profen").
Medication Dispense Record	The identity and quantity of the actual medication product dispensed by a pharmacy, physician, or over-the-counter outlet, as well as the dosing instructions provided with the dispensed medication, and any refill allowances granted by the dispenser
Medication List	A record of the set of medications that a person takes regularly. Medication lists typically include the identity of each medication, as well as specific information about when and how to take the medication.
Medication Prescription	The identity of a medication, the amount to be dispensed, the dosing instructions, and any refill allowances as specified by the prescribing physician
NDC Code	A code assigned in accordance with the National Drug Coding (NDC) system. NDC codes correspond to individual drug products on the market, and identify the specific manufacturer, drug formulation, and product packaging of each drug product. NDC codes are typically used by pharmacies, pharmacy benefit managers, and payers to track and communicate information about medications.
Personal Health Application (PHA)	A computer application that consists of alerts, reminders, condition-specific data modules, health risk appraisals, trending and other analytic tools, and other modules that help translate personal health data and medical knowledge into information that helps people make sound decisions and take appropriate action. PHAs often use data stored in Personal Health Records.
Personal Health Record (PHR)	An electronic record of data and information that is specific to the health and well-being of an individual. PHRs may contain data entered directly by patients, loaded from monitoring devices used by patients, entered directly by health care professionals, or imported from external electronic sources maintained by health care professionals (such as EHRs or laboratory systems).
PHR	See "Personal Health Record"
Pharmocogenomic profile	A profile of an individual's genome (i.e., the characteristics of her DNA and genes) that influence the action, effectiveness, and adverse effects of specific medications.
Record Custodian	The person who controls access to a Personal Health Record and performs other administrative functions. The Record Subject is often the custodian of his own record, although a record may have additional or alternative custodians (such as a parent, in the case of a young child, or a child, in the case of an elderly parent).
Record Subject	The person to whom the information in a Personal Health Record corresponds. The record subject typically has access to her personal health record, but other users may also require and be granted access.
Refill	The replenishment of the supply of a specific medication by a patient. A limited number of refills is typically authorized by a physician in the course of writing a prescription, to allow patients to replenish their supply of the medication at a pharmacy without need for a new prescription.

Registry	A directory of objects known to the Personal Health Record System, used to store and share information about those objects, as well as to maintain an official list of recognized objects. Registries may store lists of recognized users, personal health applications, data sources, etc.
Repeating Calendar Event	An aggregation of multiple calendar events that may be created, modified, or deleted together. For example, a medical appointment that is scheduled to occur every Monday for a period of six weeks would be represented by a repeating calendar event that aggregates six individual calendar events.
Role	The relationship of a specific user to a specific patient record. Roles may include "Record Subject" (the patient himself), "Family Member", "Physician", etc. One user may have different roles with respect to different patient records (e.g., "Record Subject" for her own record, and "Family Member" for a child's record), or multiple roles with respect to a single patient record (e.g., both "Family Member" and "Physician").
Therapeutic Class Hierarchy	A hierarchical classification system that groups specific medications into therapeutic or chemical classes (such as "Pain Relievers" or "Aminoglycoside Antibiotics").
User Account	A record corresponding to a registered user of a Personal Health Application. User accounts may exist for patients, family members, caregivers, health care professionals, and other parties. A user account typically consists of a unique identifier (i.e., username), other identifying information (such as last name, address, etc.), and authenticating information (such as a password or biometric profile).
XML	eXtended Markup Language. A standard syntax for representing hierarchically organized information in text files.