

OneHealthPort

# Healthcare IT Common Capability Model

High-Level Capability Model for Various Healthcare Scenarios

Dwayne Taylor - OneHealthPort  
7-15-2020

## Overview

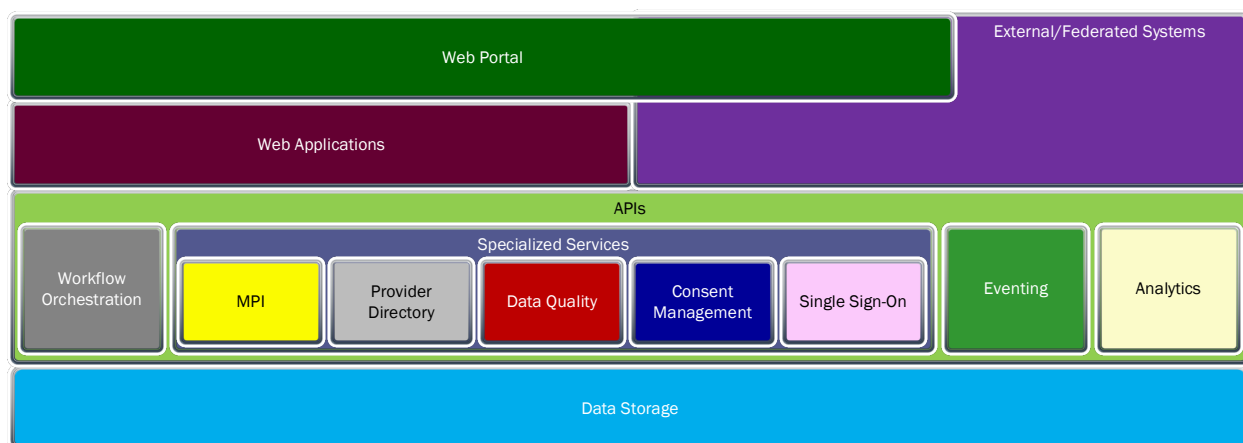
This document describes a high-level capability model for a variety of Healthcare IT (HIT) scenarios. It is not intended as a capability model at an enterprise level, as this would require the inclusion of more mundane capabilities and services to support the day-to-day operation of the business. The model is articulated very much from the perspective of a Health Information Exchange (HIE) perspective that focuses on providing capability at a community or ecosystem level rather than at an enterprise level.

The intent of this model is to identify a common set of capabilities and services used in HIT solutions in a technology-agnostic fashion. The model can be used for a variety of purposes, including but not limited to:

- Managing and understanding an organization's HIT capability inventory
- A common vocabulary to use when describing a high-level HIT solution design

## Capability/Service Model

The model is expressed as a layered set of capabilities that can be selected for the composition of a solution to solve a given problem. Not all capabilities are required to solve a given problem; conversely, not every capability is required to solve any given problem. The capabilities are described as such to be technology- and implementation-agnostic. For example, a Workflow Orchestration capability is intended to describe a technology capability that can be used to fulfill a specific need but does not imply a specific implementation, whether it's Azure, AWS or an on-prem vendor product. Also, the model does not imply that the components be hosted in a centralized model within the same environmental boundaries. Assuming that the implemented capability supports standards-based interoperability, it is assumed that they could be distributed across multiple environments, potentially hosted by different organizations.



## Components

- **Web Portal.** The web portal is an aggregation point for various web applications, whether it provides a link to external one or to one hosted on the platform. Also, external applications, such as EHR systems can have provisioned access to specific services at the API layer. A standardized approach to identity and access management is established and leveraged for all applications hosted within the portal on the platform.

- **Web Applications.** Web applications are those user-facing applications that are hosted internally on the platform. With each service that is implemented in the platform, it should be evaluated as to whether or not a proprietary user interface belonging to a specific service should be leveraged as a federated application on the portal or if the user-facing functionality of the service should be integrated into a single user interface.
- **External/Federated Systems.** These are various systems and services external to the scope of a given organization or solution that may still interact with capabilities in scope of the model. Examples of external systems can be fairly extensive, including Electronic Health Record (EHR) systems, external MPIs, consent management systems, etc.
- **APIs.** Unless by exception, the platform uses an API-first approach to expose services and data.
- **Workflow Orchestration.** Unless leveraging the “secret sauce” of a specialized service, a robust but generic workflow orchestration engine should be capable of enabling various scenarios where a workflow needs to be orchestrated across multiple users, independent components within the platform, or with external applications.
- **Specialized Services.** Specialized services are those that would be difficult or cost-prohibitive to build in-house due to specialized knowledge of technology or business, or simply because the level of effort would be considerably greater to build it custom rather than leverage one someone else has already built. This stands in contrast with commodity services, such as data storage, API management and workflow orchestration.
  - **MPI.** An MPI is the authoritative source for a given patient population and exposes a service that can be used to match patients based on provided demographics and identifiers
  - **Provider Directory.** A provider directory is the authoritative source for a provider population and exposes a service that can be used to match providers based on demographics and identifiers
  - **Data Quality.** Orthogonal to a consent management solution but an important platform component overall, a data quality service can be leveraged to clean up clinical data and generate several useful data products from it.
  - **Consent Management.** A consent management solution is considered a “specialized service” in the platform because it assumes that the functions of consent management are difficult to easily and accurately replicate using commoditized technology components. It’s also important to note that in the bigger picture, a consent management solution is one component in a larger ecosystem and is not the heart of the ecosystem.
  - **Single Sign-On (SSO).** A Single Sign-On service provides the ability to centrally manage identities and access for users as not to require a separate login for each web application that is accessed. Examples of SSO services include OneHealthPort’s SSO service and Secure Access Washington (SAW).
  - Other specialized services can be added as needed to implement specific kinds of services

- **Eventing.** An eventing component is important for implementing services that leverage an Event-Driven Architecture (EDA). It enables the publication of significant events in real-time. Concerned parties who deem the events to be significant can subscribe to them and be notified when they occur. Events contain relevant data to retrieve from APIs or to interact with workflows depending on the event in question.
- **Analytics.** Analytics provides a way to understand system behavior, the flow of data and business indicators in an aggregate fashion.
- **Data Storage.** Data storage takes various forms to persist raw files, documents and relational data.

## Example Solution Architecture

Using the capability model described in the previous section, one can identify the required capabilities to support a particular solution using a technology-agnostic approach. For example, if one were looking to implement a clinical data repository (CDR), one might incorporate the following components:

- A Single Sign-On (SSO) solution for identity and access management of users,
- A Web Portal with functionality to search and view clinical data for users,
- A Set of APIs to provide backend functionality for the Web Portal (assuming API first development best practices are being observed) and for direct system-to-system interactions between organizations other systems and for workflow automation.
- A Workflow Orchestration/Automation solution to manage the automated the ingestion of data
- An Eventing capability to notify interested parties when a particular event has occurred with the data, such as a reportable health condition, COVID, or a variety of other triggers for notification.
- A Master Patient/Person Index (MPI) to ensure that patient information can be consistently resolved to a single individual
- A Consent Management solution to manage visibility of sensitive data such as that regulated by 42 CFR for consumption in an identifiable format.
- Various forms of data storage to support the persistence of data.

This exercise could be taken a step further to define the specifics for an implementation; however, the intent of the model is to provide a framework in which HIT capabilities can be commonly enumerated for organizational capability management and high-level solution design.