PATIENT UNIFIED LOOKUP SYSTEM FOR EMERGENCIES (PULSE)

March 16, 2015
Prepared for the Office of the
National Coordinator for Health IT

Prepared by:
Scott Afzal, Principal
Genevieve Morris, Director
Sandeep Antony, Solutions Architect
David Minch, President/Board Chair, CAHIE
Rim Cothren, Executive Director, CAHIE

Audacious Inquiry, LLC
5523 Research Park Drive, Suite 370
Baltimore, MD 21228
301-560-6999

Introduction

After a major disaster, individuals are displaced from not only their homes but also from their primary care providers and local hospitals, sometimes leaving behind needed medications, and almost always leaving behind pertinent medical records. Hospital patients in affected areas are typically transferred to hospitals outside of the area, and individuals who sustain injuries must be triaged and treated appropriately. Providers and first responders who are treating these individuals often work with incomplete medical information, which is ineffective and potentially unsafe. In 2014, the Office of the National Coordinator for Health Information Technology (ONC) and HHS Office of the Assistant Secretary for Preparedness and Response (ASPR) collaborated to evaluate how health information exchange (HIE) could be used in times of disaster to provide safer more effective care to individuals. One of the recommendations from this collaboration was the development of a disaster response medical history portal called the Patient Unified Lookup System for Emergencies or PULSE. PULSE could be activated during and after a disaster and provide users with a summary view a patient's medical history.

In late 2014, ONC and ASPR received a joint HHS Ventures award, through its innovative IDEA Lab, to begin to lay the foundation for PULSE in California. The award provided for the beginnings of a pilot of PULSE in California through the development of a detailed use case, technical architecture, and an evaluation of policy considerations. Ultimately, PULSE can be made available in any geographic area to support healthcare professionals and first responders caring for displaced individuals or volunteer healthcare workers are deployed to a disaster area to care for victims outside of their normal health IT environment. As such, the technical specification could work with existing California infrastructure or be deployed in other geographies. Additionally, the pilot takes a phased approach to the capabilities available in PULSE, with the initial roll-out envisioned as a simple query and retrieve for Consolidated-Clinical Document Architecture (C-CDA) documents. Future phases may offer additional functionality, including an ability to query for more granular health information and consolidate multiple responses, a centralized registry for tracking displaced individuals, the ability to record data on the treatment provided to the patient (i.e. basic electronic health record functionality), and the ability to send data collected in PULSE to a receiving provider and/or the patient's home provider. The use case and technical specification both note the planned phasing of capabilities. This report details the use case (an earthquake affecting California), policy considerations that will need to be addressed in future phases, and the technical architecture envisioned for PULSE.

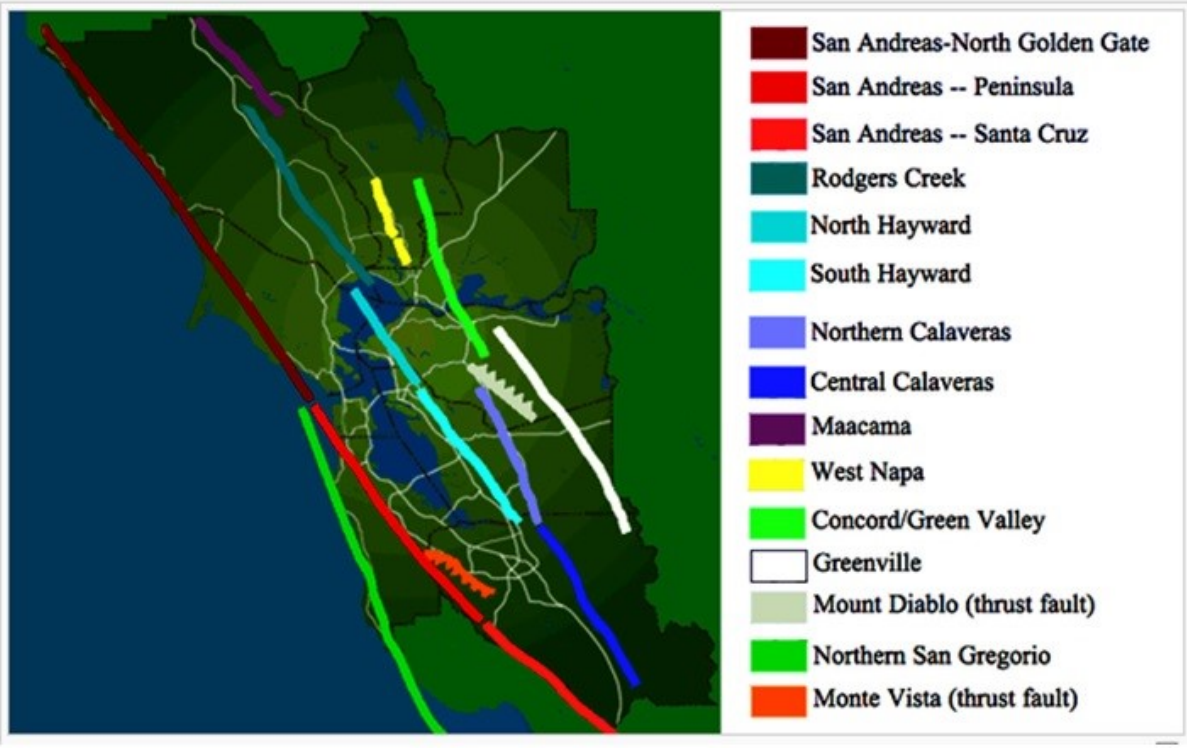
The project team (including Audacious Inquiry and the California Association of Health Information Exchanges (CAHIE)) worked with ONC, ASPR, and the California Emergency Medical Services Agency (CalEMSA) to identify a list of organizations interested in participating in PULSE. These organizations were asked to sign a letter of intent to participate in the pilot program.

Use Case

Earthquake Scenarios

San Francisco Bay Area Faults

The PULSE pilot use case focuses on the San Francisco Bay Area.



A magnitude 7+ earthquake on the South Hayward Fault is the most reasonably expected event, since the last major event was in 1868, and the fault averages 140 years between earthquakes. A U.S. Geological Survey (USGS) of the Southern Hayward Fault indicates an 11.3 percent probability of a 6.8 magnitude earthquake in the next 30 years, directly affecting 5 million people in the San Francisco and East Bay.[1] The South Hayward Fault is connected to the North Hayward and Rogers Creek Faults (with offset) under the San Pablo Bay – none of which have had any recent activity – the recent Napa quake was on the West Napa Fault to the east of the Rogers Creek Fault.

The use case disaster scenario described is a 7.2 magnitude earthquake on the South Hayward Fault (light blue in the map above), followed shortly (2 days) by a 6.5 magnitude secondary slippage on the North Hayward and Rodgers Creek Faults (linked but separate faults to the north of the South Hayward Fault). Such an earthquate would impact most of the western portions of Alameda and Contra Costa, and Southern Napa and Sonoma counties. A quake on the South

[1] http://earthquake.usgs.gov/regional/nca/wg02/losses.php

Hayward Fault would leave evacuation routes to the north and west generally intact, with the possible exception of Route 580 between Castro Valley and Dublin. Assuming that the new eastern span of the Bay Bridge structure meets the 8.0 standard it was designed to withstand, the only additional impact of the other quakes would be to temporarily shut down the Carquinez Bridge (Highway 80 N out of Richmond), which puts more pressure on the Benicia Bridge.

The use case assumes that most of the emergency services capacity in Alameda County will be impacted as well as at least 50 percent of the available hospital beds in both Alameda and Contra Costa counties. Evacuation routes are Route 101 to the North and South out of San Francisco, Route 80 to the north and Route 24 east for Richmond, Berkeley, and Oakland, Route 680 north to 80 (over the new Benicia bridge) for most of Contra Costa, and traffic from Oakland and Berkeley over Route 24. Route 580 East for Hayward, San Leandro, and Fremont, and 680 N to 580 or 680 S to 101 for San Jose.

Populations	*Affected*	*Displaced*
Alameda (60%)	1.6M	960,000
Contra costa (30%)	1.1M	330,000
San Francisco (10%)	0.8M	80,000
San Mateo (5%)	0.7M	35,000
Santa Clara (10%)	1.8M	182,000
Total	**6.0M**	**1.587M**

Since there is very little major infrastructure down the 101 corridor, the use case assumes that the major flow of displaced and injured will be to the north and east, with the vast majority (assume 1.3 million) ending up in the central valley between Modesto and Sacramento. The above scenario, assumes establishment of emergency medical capabilities (MHOAC and RDMHS) at Fairfield (Solano County), Sacramento (Sacramento County), Stockton (San Joaquin County), and Modesto (Stanislaus County).

Evacuation Routes & RDMHS

Triage and Treatment Shelters

Earthquake epicenter and damage areas

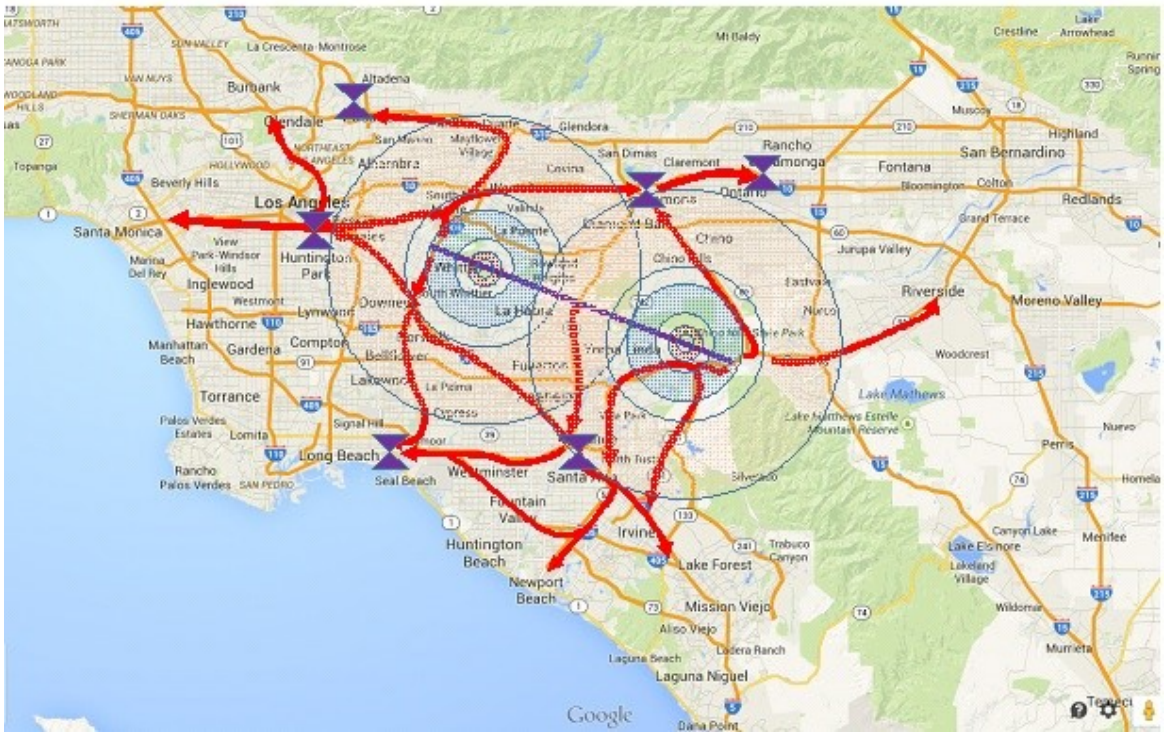
Whittier Fault and Upper San Jacinto Fault Zone in Sothern California

For the Southern California earthquake scenario, either the upper San Jacinto or the Whittier Faults could be devastating events, if the quakes are deep and propagate. While neither is part of the San Andreas Fault, which lies further to the east, the San Jacinto Fault is part of the plate fracture zone and hence could be part of a more massive event on the San Andreas Fault. For that reason, the use case concentrates on the Whittier Fault because it is relatively isolated (it is at the top of an associated but not connected fault line called the Elsinore Fault Zone). A significant event of 7.2 magnitude is likely on the Whittier Fault, which has not had a major slippage since records have been kept. The Whittier Fault is bounded by the Pomona Freeway to the North, San Diego, I5, and Riverside to the South and East, the 71 to the East, and 605 to the West.

If a seismic event occurs on this fault, significant damage would occur to the cities of Pico Rivera, Whittier, La Habra, La Mirada, Brea, and Yorba Linda. Secondary but significant damage would occur to Fullerton, Placentia, Buena Park, Downey, Norwalk, and Anaheim (which would impact Disneyland and consequently a large number of individuals). Evacuation routes will most likely be as shown below, assuming that the freeway system stays generally intact – populations to the North of the fault will travel north and east toward Pomona, San Bernardino, and Riverside; populations to the south will travel south and west toward the downtown area and toward Newport and cities to the south.

Populations affected will be roughly similar to those projected for the northern California earthquake, with roughly 5 million in the affected region of the quake, and likely 1.5 million displaced. The major impact will be to portions of Los Angeles, Orange, Riverside, and San Bernardino counties (total population of 17.5 million), with some patient spillover to Ventura and potentially Kern and Santa Barbra counties (population of 2 million).

Hypothetical Triage and treatment centers would be located immediately outside the major areas of disruption, near major tertiary care facilities and trauma centers which have been seismically reinforced. We will again assume, as is true for the northern California scenario that most of the hospitals in the primary and secondary zones will be either partially or completely incapacitated and will require evacuation, or will at the very least, not have the ability to take new patients.



Triage and Treatment Shelters

Earthquake epicenter and damage areas

CalEMSA Earthquake Use Case for Investigation

Preconditions

- In each disaster location (northern California and southern California), there are an adequate number of triage and treatment center resources for establishing the proposed centers – each scenario proposes six centers.
    - Three of the proposed centers at each location are located at fairgrounds or arenas where there is a large open parking space and adequate space for erection of field hospital resources.
        - Each field location has adequate power availability or generator assets and all other required infrastructure.
        - Each field location is either pre-equipped with high-bandwidth connectivity to the internet or has a plan for erection of a mobile 2-way satellite link for internet service.

  - Each field location is supplied with an adequate number of tablets and other portable workstations, which can be used to obtain patient data and document care.[2]
  - Each field location is licensed for an EHR technology that can be used to document treatment.
  - Each field location's EHR is connected to an HIE technology, which can be used to make recorded treatment data available upon transition of care.
  - Each field location (either through the EHR technology or as a stand-alone resource) has connectivity to the California Trusted Exchange Network (CTEN) and to the CalEMSA single sign-on (SSO) functionality and the emergency worker's registry (commonly known as the ESAR-VHP database in other states which is named DHV in California for Disaster Healthcare Volunteers).
- Three of the proposed centers at each earthquake location are associated with large tertiary care hospitals or trauma centers.
  - Each hospital location has adequate power availability or generator assets and all other required infrastructure.
  - Each hospital location has unrestricted connectivity to the hospital's internet link – this might require pre-configuration of the hospital's firewalls for an emergency hook-up.
  - Each hospital location is supplied with an adequate number of tablets and other portable workstations, which can be used to obtain patient data and document care (should be part of the hospital's disaster preparedness plans).
  - Each hospital location will be staffed by hospital workers or emergency personnel who are pre-qualified to work with the hospital's EHR. An alternative to this would be the use of the field location EHR as noted above.
  - Each hospital location's EHR is connected to an HIE technology which can be used to make recorded treatment data available upon transition of care.
  - Each hospital location's EHR is connected to the CTEN.
  - Each hospital location, if the field location EHR and HIE is used, also has connectivity to the CalEMSA SSO capability and the emergency worker's state registry (DHV database).

[2] The project team assumes that all affected hospital systems and primary care offices have adequate backups for their EHRs and have adequate plans for their networks to be able to access them in emergent situations (both of which are required under HIPAA). One remaining question is where to get workstation devices and bandwidth for the field. Judicious agreements with large chain stores that sell such devices could potentially cover all of California as an example (think of it as a pre-purchase contract that gives the emergency centers preferential access to their inventory). Bandwidth, could be accomplished with pre-engineered rolling network centers (something that would have to be developed, but clearly not necessary for the pilot phase.

- A significant portion of the hospitals and primary care medical offices and clinics in the impacted areas are using operational EHRs that either also have embedded HIE functionality or that are, in turn, connected to an enterprise-based or community-based HIE.
- A significant portion of the hospitals and primary care medical offices and clinics in the impacted areas have HIE assets either directly available on the CTEN, or made available through a CTEN participant. In short, the pilot prerequisite requirement is that patients and the general public who are displaced have their records available for access through the CTEN.[3]
    - NOTE: The CTEN is required for use of the California Directory Services and for interoperation using both Direct and Exchange protocols. If the only protocol to be used is Exchange, then connectivity to either the CTEN or the eHealth Exchange would be sufficient.
    - NOTE: Availability on the CTEN means that:
        - Organization has signed the CalDURSA
        - Organization has on-boarded with each of the protocols expected to be used (for purposes of the use case, the three protocols are Direct, Exchange, and Directory Services).
- For hospitals in the primary impacted areas, which are not capable of continuing operations, their patients will be evacuated using available transport resources (not necessarily ambulance or typical emergency transports) with hospital identification bands intact.
- CTEN Directory services is pre-loaded with the path to every participating California hospital's patient data query service URL (HIE or EHR with HIE functionality).
- CTEN Directory services is pre-loaded or federated to the Direct directory service of all participating California primary care organizations (HIE or EHR with HIE functionality).

Use Case Workflow

There will be five classes of refugees from the primary and secondary impact zones which will become patients of the disaster locations:

1. Evacuee patients from non-functioning and over-burdened hospitals;
2. Severely injured who will be transported by emergency vehicles;
3. Ambulatory injured who will transport themselves or will be brought by non-emergency means requiring triage for emergent care;
4. Minimally injured who are in need of urgent care (sprains, hypertension, etc.); and
5. Uninjured refugee evacuees requiring shelter, connection to social services, connecting to family members etc.

[3] For states other than California, the underlying assumption is that PULSE would connect to HIE infrastructure where it does exist and act as the infrastructure where it does not currently exist.

6. Uninjured refugee evacuees requiring general primary care for after-event and/or chronic illnesses and prescriptions / refills.

The team will take a phased approach to developing and implementing PULSE, with the pilot phase focusing on query and retrieve of C-CDAs, and future phases expanding PULSE's capabilities to include a central disaster registry and other functionality. The phases are noted in the following workflows.

Class 1: Patients evacuated from other hospitals

These patients will be transported to other functioning hospitals capable of taking additional patients. The area and county disaster plans will maintain an inventory of open beds allowing transports to distribute patients appropriately. When patients arrive, they will be identified by hospital and MPI from the arm or ankle band. If all available beds are filled, patients may be taken to field hospitals.

Phase 1: Pilot

1. Source hospital will be selected in the search screen.
2. Patient's MRN and last name will be scanned from the ID band or key-entered.
3. Patient and document query made to the hospital's query service (patient is explicitly known).
4. Identifying information and document list returned.
5. CCDA summary of care (may be a CCD, discharge summary, or other document template) obtained for the Patient. PULSE will provide a style sheet to render CCDAs into human readable format.

Phase 2

6. CCDA summary of care (may be a CCD, discharge summary, or other document template) for the patient consumed into the Disaster EHR Portal or the host location's EHR Demographics
7. A disaster encounter identifier is issued from a central authority and together with the patient's name and demographics a device-readable armband is printed and affixed.
8. A registration message is sent (Direct) to the CalEMSA Disaster Registry (CalDReg)
9. Treatment commences with documentation in the host EHR or the Disaster EHR Portal.
10. Upon discharge or transfer to another site, a discharge message is sent to the CalDReg and an identification card is printed for the patient with a QR code. This card can be used to easily re-identify the patient at their next encounter.
    - If we wanted to get more sophisticated, the QR code could be coupled with a finger scan on the issuing device which can be encoded and sent to the CalDReg to be used to uniquely Id the patient and eliminate misuse or fraudulent use.

Class 2: Severely injured patients transported by emergency vehicles

These patients will arrive at hospital emergency rooms or field hospitals requiring immediate treatment or triage to other emergency care locations. Patient identity and the search for previous records may start with the patient's recollection of their last medical encounter at either their local hospital or their primary care physician, or may begin with a broadcast query to all facilities participating in PULSE. Whenever possible, the patient's insurance card or ACO/HMO member card should be obtained since that can give an immediate link to the patient's records.

Phase 1: Pilot

1. Patient's driver's license or state ID card and their insurance or ACO/HMO member card is obtained. If this information is available, a specific query can be placed to a specific institution. Go to step 3 above.
2. If no information (or suspect/unreliable information) is available on the patient's person, then anecdotal information about the patient is obtained from third parties (location where injury occurred), patient name, and other clues to identity.
3. Patient discovery is broadcasted to all PULSE participants. Data search and additional dialogue needed to uniquely identify the patient.
    a. If the patient's records are eventually found, proceed to step 5 above

Phase 2

4. Patient's records are not found: begin a new chart for the patient using initial information from the most reliable sources. Search for the patient in the CalDReg. If the patient is found, enter the UniqueID information into the registration and proceed to step 8 above.
    - If the patient is not found, proceed to step 7 above.

Class 3: Ambulatory injured patients; self- or other- transported by non-emergency vehicles

These patients will arrive at hospital emergency rooms or field hospitals requiring triage to urgent or emergency care. Patient identity and the search for previous records starts with the patient's recollection of their last medical encounter at either their local hospital or their primary care physician. Whenever possible, the patient's insurance card or ACO/HMO member card should be obtained since that can give an immediate link to the patient's records.

Phase 1: Pilot

1. Patient's driver's license or state ID Registry is searched for the patient's last encounter location (PCP or Hospital).
2. Skip to step 3 above.
3. Patient's Primary Care Physician name and location is obtained from the patient or their ACO/HMO card or insurance card.
4. Location is chosen from a list on the CTEN Directory Search screen.
5. If patient does not know this information, patient discovery is broadcasted to all PULSE participants. Data search and additional dialogue needed to uniquely identify the patient.
    a. If the patient's records are eventually found, proceed to step 5 above
6. Go to step 3 above.

Class 4: Non-injured or minimally injured who are in need of urgent care

These patients will arrive at field hospitals or urgent care sites requiring treatment for minor injuries or anxiety. Patient identity and the search for previous records starts with the patient's recollection of their last medical encounter at either their local hospital or their primary care physician. Whenever possible, the patient's insurance card or ACO/HMO member card should be obtained since that can give an immediate link to the patient's records. These patients will follow the process outline for Class 3 patients above.

Class 5: Uninjured refugee evacuees requiring shelter and general primary care

These patients will arrive at field hospitals or clinics requiring general primary care. These patients will follow the process outlined for Class 3 patients above.

Post Conditions

At this point it is unknown how long the use case is to be deployed; consequently, it is difficult to determine what (other than disaster resolution and shutdown) the end-state is expected to be. It is expected that there will be an ability to track patients receiving care through this process regardless of where they settle, or seek care after the disaster scenario completes.

Policy Considerations

Declaration of an Emergency

The current vision of PULSE is that it would activate during a disaster or emergency declaration to enable treatment of patients who are displaced from their primary medical providers and provide a utility to disaster workers who are displaced from their normal systems. While ultimately a system such as PULSE should always be available (since patients seek medical treatment across geographies), to get the most participation, the initial scope of PULSE will be focused on use after a disaster, specifically the use case described above. As PULSE is developed, effort will be made to get agreement amongst participants to keep PULSE "turned on" and available before, during, and after disasters, though this will be dependent on participants. Disasters or emergencies can be declared at a number of levels: city, county, state, national, etc. The level of emergency declaration that activates PULSE was not discussed or decided on during this phase of the project. However, the project team believes that each participating entity may need to decide when to activate PULSE. The team posited that this may be included in the participation agreements signed by organizations to enable their participation in PULSE.

Patient Consent

The Health Insurance Portability and Accountability Act (HIPAA) governs the exchange of patient data, including sharing for treatment, payment, and operations, and 42 CFR Part 2 governs the exchange of alcohol and substance abuse treatment information. States may impose additional privacy regulations that may be stricter than HIPAA and 42 CFR Part 2. There is significant variation across states regulations, particularly relating to patient consent to share information. While some states take an opt-in approach (data is only shared if the patient proactively agrees to have it shared), others use opt-out policies (data is always shared unless a patient indicates they do not want data shared), which typically include "break-the-glass" rules on exchanging health information during an emergency. The perception is that this variation across states makes sharing data across state lines difficult. Additionally, as data is shared electronically, there is a need for the patient's consent to share the data to persist, so that providers who are receiving the data know whether they can further share it, and so on. At a national level, the concept of consent is in flux and may change in the near-future.[4]

Also, the S&I Framework, working with ONC and SAMSHA is developing Consent2Share architecture, which includes a front-end, patient facing system known as Patient Consent Management (PCM) and a backend control system known as Access Control Services (ACS).[5] These technical standards are meant to persist patient consent as data is shared. The project is

[4] Connecting Health and Care for the Nation A Shared Nationwide Interoperability Roadmap Draft Version 1.0. Office of the National Coordinator for Health IT. January 2015. http://www.healthit.gov/sites/default/files/nationwide-interoperability-roadmap-draft-version-1.0.pdf

[5] http://wiki.siframework.org/SAMHSA+Consent2Share+Project

currently piloting the standards, which may be available for wider use in the near future. These standards are not included in the current architecture, but may be added into Phase 2 as they become available. For purposes of the pilot, PULSE participants would rely on existing participation agreements and internal policies to determine consent policies.

Sustainability and Ongoing Funding

Initial funding for the PULSE design project was obtained by ONC and ASPR through the HHS Ventures IDEA Lab. However, there is a need for ongoing funding to support the infrastructure necessary to activate PULSE during an emergency declaration or disaster. More research is needed on private, federal, and state funding levers to support the ongoing operation of PULSE.

Workflow

The initial rollout of PULSE will include the query and retrieval of C-CDA documents, which may be a CCD, discharge summary, history and physical, etc. These documents are meant to be a summary of the patient chart, but they are often very long and include a full history of lab results, procedures, and other patient information that may not be applicable to treatment of the patient, particularly in this use case. This introduces workflow issues for the providers and first responders treating the patients, since they would have to look through potentially hundreds of pages to find clinically relevant data, such as the medication or allergy list. There is a need to work with providers and first responders to determine the most valuable data elements from a patient's historical record. Once the list is determined, an HTML overlay should be built to pull out the most important data elements and present them to the users in a human readable format. Future phases of PULSE could allow for the query of specific data elements, such as medications or allergies, which may help to resolve the workflow issues.

Identity Proofing Levels

The technical architecture includes incorporation of BlueButton data into PULSE. One potential source of BlueButton data is the Centers for Medicare and Medicaid Services (CMS), which provides BlueButton capabilities to Medicare beneficiaries. For individuals who do not have data in one of the participating healthcare organizations, CMS may be a vital source of information. While traditionally BlueButton has been used to make data available to individuals, the BlueButton API that is currently under development could be used by PULSE to allow providers to access BlueButton data from CMS when other data is not available on the patient. This use of BlueButton would require that the provider using PULSE be authenticated and authorized to access the data. CMS requires authentication and authorization be Fair Information Practices (FIPS)-compliant. Consequently, there will need to be assurances that all participants in PULSE are utilizing the same identity proofing and authentication levels that are FIPS-compliant, if CMS data is to be used.

Summary

This document lays out a number of policy considerations that will need to be addressed prior to implementation of PULSE. In addition, the technical architecture described in the next section is fairly high level, and detailed technical specifications will need to be drafted based on the

technical capabilities of PULSE participants. Finally, additional participants in California and other states will need to be engaged to ensure a high availability of patient data.

Technical Architecture

Summary

When natural or manmade disasters occur, individuals are often displaced from their homes and consequently from their healthcare providers, leaving them to seek medical care from providers they likely have not had previous experience with. Additionally, the area's medical system is often stretched beyond its limits during a disaster, and volunteers are placed in these areas to care for individuals, meaning that patients will be seeking care from those that do not have access to the primary systems where their records are kept. Consequently, individuals' health information, including medications, allergies, problems, etc. is often unavailable to the providers caring for them during or after a disaster, leading to suboptimal care and potential patient safety issues. To support the retrieval of individuals' health information during a disaster, ONC has partnered with the Office of the Assistant Secretary for Preparedness and Response (ASPR) to develop and deploy PULSE in the state of California. PULSE will comprise a set of services – services to establish organizational and system authentication, to discover information resources and other services, to authenticate disaster workers, to identify patients, and to search for and retrieve health information – designed to be accessed through a portal in time of disaster. In California, some of these services are currently embodied in the California Trusted Exchange Network (CTEN) and some through the Disaster Healthcare Volunteer (DHV) database. In other geographies, existing infrastructure may exist that PULSE can rely on for some of these services, in other areas infrastructure may not exist. Consequently, the technical architecture described is intended to be generalizable to other geographies and can work with infrastructure where it exists and provide the infrastructure where it does not exist.

Purpose

The purpose of this architecture document is to describe the following aspects of the PULSE solution:

- Business context and use cases identifying business needs;
- Application Architecture components identifying communication protocols and interfaces;
- Data architecture which identifies the data elements being managed by the system;
- Technical architecture for implementation; and
- Security Architecture of the system.

Audience

The intended audiences for the architecture document are stakeholders who will champion the development and implementation of the PULSE solution. It will also describe the integration options for HIOs and health systems.

Scope

The PULSE system is designed to provide healthcare professionals caring for displaced persons with medical conditions with consistent, concise individual document representations of individuals' health information which may be drawn from disparate systems in the region, in case of major disaster event. The disparate systems could include HIOs, health systems, ambulatory practices, emergency medical service agencies, etc.

Related Documents

The following is a list of related documents that were used as references to produce the architecture document.

- HIE for Disaster Response[6]
- PULSE Earthquake pilot scenario supporting information
- California Data Use and Reciprocal Support Agreement (CalDURSA)

Solution Overview

Objectives

- PULSE is available when a state of emergency is declared.
- PULSE will allow healthcare professionals registered with ESAR-VHP (referred to as Disaster Healthcare Volunteer (DHV) For California's program), healthcare professionals who work for a participating health system, and healthcare professionals who participate with an HIO access to patient data.
- Healthcare professionals will be able to search for patient data by patient demographics, such as name, date of birth, address, phone number, etc.
    - If a patient is transferred from a facility, then the facility identifier will be included in the query.
- PULSE will broadcast a query to all its members checking if patient data exists.
- PULSE will prefer to retrieve patient summary in C-CDA format when possible.
- All activities in PULSE will be tracked through an audit log.

Constraints

The design of the PULSE system is constrained by the following needs:

- The solution model should be easy to replicate across other regions in within the nation.

[6] Health Information Exchange Services in Support of Disaster Preparedness and Emergency Medical Response: Assessment of Opportunity in California and the Gulf Coast. Scott Afzal, Genevieve Morris, Stephen Palmer. Prepared for the Office of the National Coordinator for Health IT under Subcontract 76-01074-000-44 to A+ Government Solutions under Prime Contract GS35F0565T/N10PD18202. April 2014. http://www.healthit.gov/sites/default/files/hiefordisasterresponse_final_04232014.pdf

- The solution should adopt nationally-available standards to drive connectivity wherever possible.
- Healthcare professionals targeted to use PULSE may come from different regions and settings, so the authentication process should be versatile to support as many groups/classes of professionals as possible.
- PULSE infrastructure should be setup in a region that is least likely to be affected by a disaster event that it is attempting to support. E.g. If the disaster region is California, then PULSE for California should be designed to operate from outside California.
- PULSE participants should make their disaster recovery endpoints available in case their primary site is down, this is a HIPAA requirement.
- PULSE will utilize existing health information networks wherever possible.

Architecture Methodology

The architecture document uses The Open Group Architecture Framework (TOGAF) methodology:[7]

- Business Architecture views dealing with the business context and use cases.
- Application Architecture views documenting the system components, their interfaces and protocols.
- Technology Architecture views showing the logical and physical deployment configurations.
- Security Architecture views documenting the critical security controls for the PULSE solution.

Implementation Guidelines

This section describes the updates to this document or additional documents that may be needed while developing, implementing and operating the PULSE system.

- Change Management Plan
- Disaster Recovery Plan
- Security Plan
- Infrastructure Component updates in Technology architecture section
- Reporting needs from PULSE

When implementing in a region that houses existing health information networks, PULSE will work with such networks. For example in the California region, PULSE will utilize DHV and CTEN.

- Disaster Healthcare Volunteer (DHV) – California's ESAR-VHP program
- California Trusted Exchange Network (CTEN) – eHealth Exchange Network in California

[7] http://www.opengroup.org/togaf/

Conceptual Solution

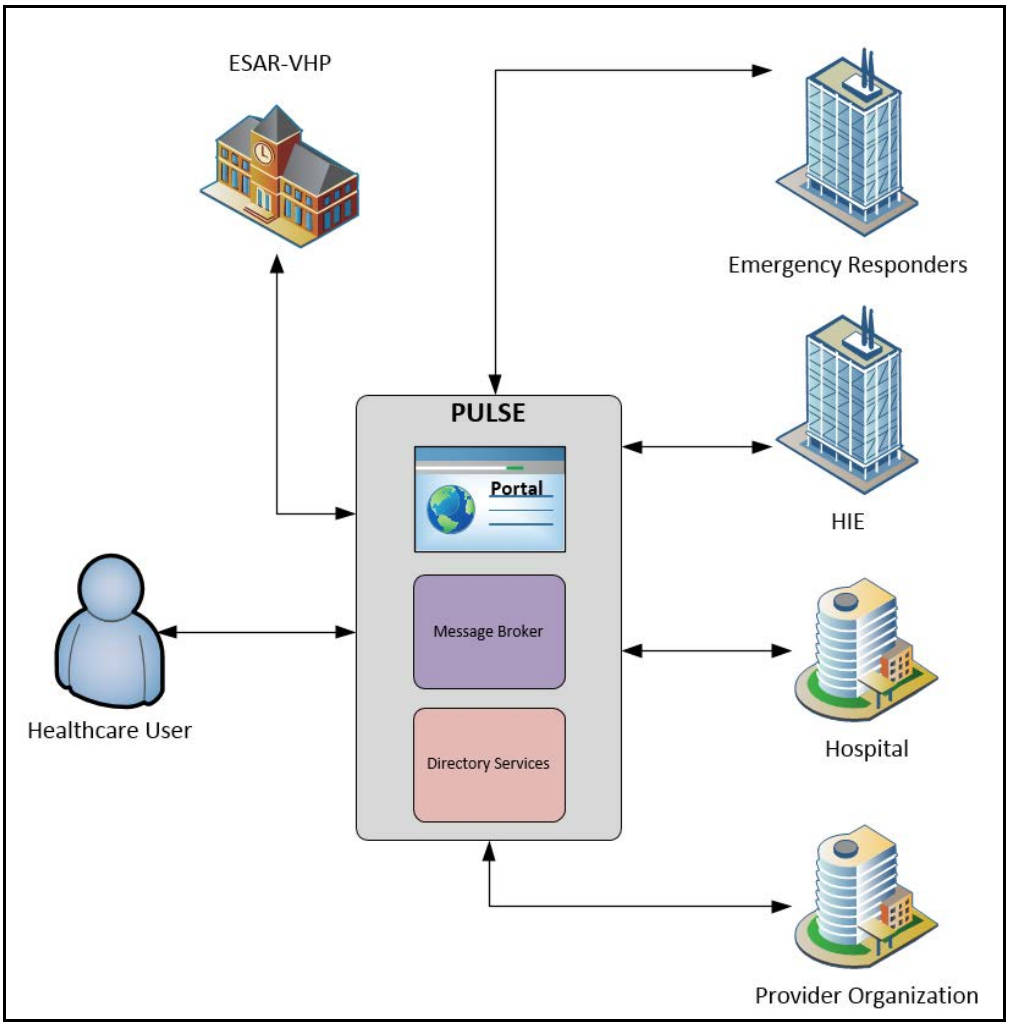


Figure 1: Conceptual Solution

Architecture

This section documents the various architecture views of the PULSE system.

Business Architecture

This sub-section captures the business architecture of the PULSE system.

Business Architecture Principles

The following are some of the critical business principles applied to analyze, prototype, design and implement the PULSE system.

- Use information technology to provide access to patient information settings and locations.

- Allow users who have accounts in ESAR-VHP or with a participating health system or HIO to access PULSE.
- Utilize national standards and frameworks to connect to disparate health systems.
- Ensure that the system is activated only when an authorized agency declares a disaster event in the region.
- Solutions are designed to ensure that users experience an acceptable response time.
- Solutions are designed to handle high volume of users and traffic.
- Ensure the PULSE system meets the security and privacy requirements of federal and state laws such as HIPAA, CMIA, and contractual requirements of the CalDURSA.
- Ensure that the technology solutions provide simple, engaging, and seamless end user interfaces.

Functional View

Decomposition View

The Decomposition View describes the business functions broken down by sub-components.

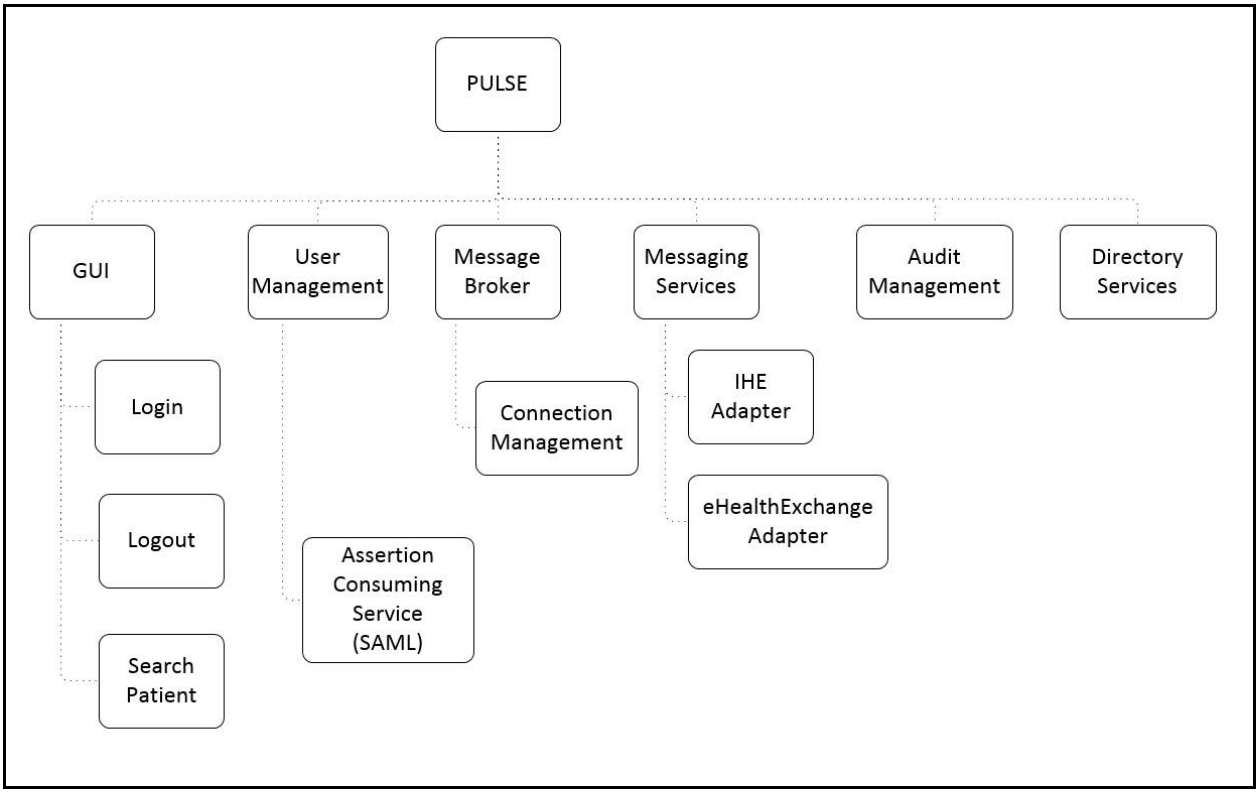


Figure 2: Decomposition View

Business Services description

The table below describes the different business services required and their categories for PULSE.

Business Service Category	Business Service	Business Service Description
User Interface	Login	This service allows users to login to PULSE.
User Interface	Logout	This service allows users to logout of PULSE.
User Interface	Search Patient	This service allows users to search for a patient providing relevant demographic information.
User Interface	Retrieve Document(s)	This service allows users to choose a patient and then select and retrieve specific summary document(C-CDA) from a specific source.
User Management	User Management	The module captures the identify information of the user from the SAML and makes it available in the user session.
User Management	Assertion Consuming Service (SAML)	This service will allow users that are credentialed by external Identity Provider systems to access PULSE. This is done by verifying the SAML assertion presented by the user request.
Broker	Message Broker	This service will interface between the frontend and the messaging services to federate and aggregate requests and responses.
Internal	Audit Management	This service will track all activity performed through PULSE.
Internal	Directory Service	This will be an internal directory for PULSE to lookup endpoints. For the California pilot, the CTEN Directory Services will be used.
Internal	Connection Management	The module will manage connection information required for PULSE to interact with Health Systems
Messaging Service	eHealth Exchange Adapter	This service will enable the client to connect to eHealth Exchange participants.
Messaging Service	IHE Adapter	This service will enable the client to connect to IHE compliant participants.

Business Use Cases

These views describe the use cases that are supported through PULSE.

Use Case 1: PULSE Portal User

This view describes a healthcare professional accessing the PULSE portal during an emergency.

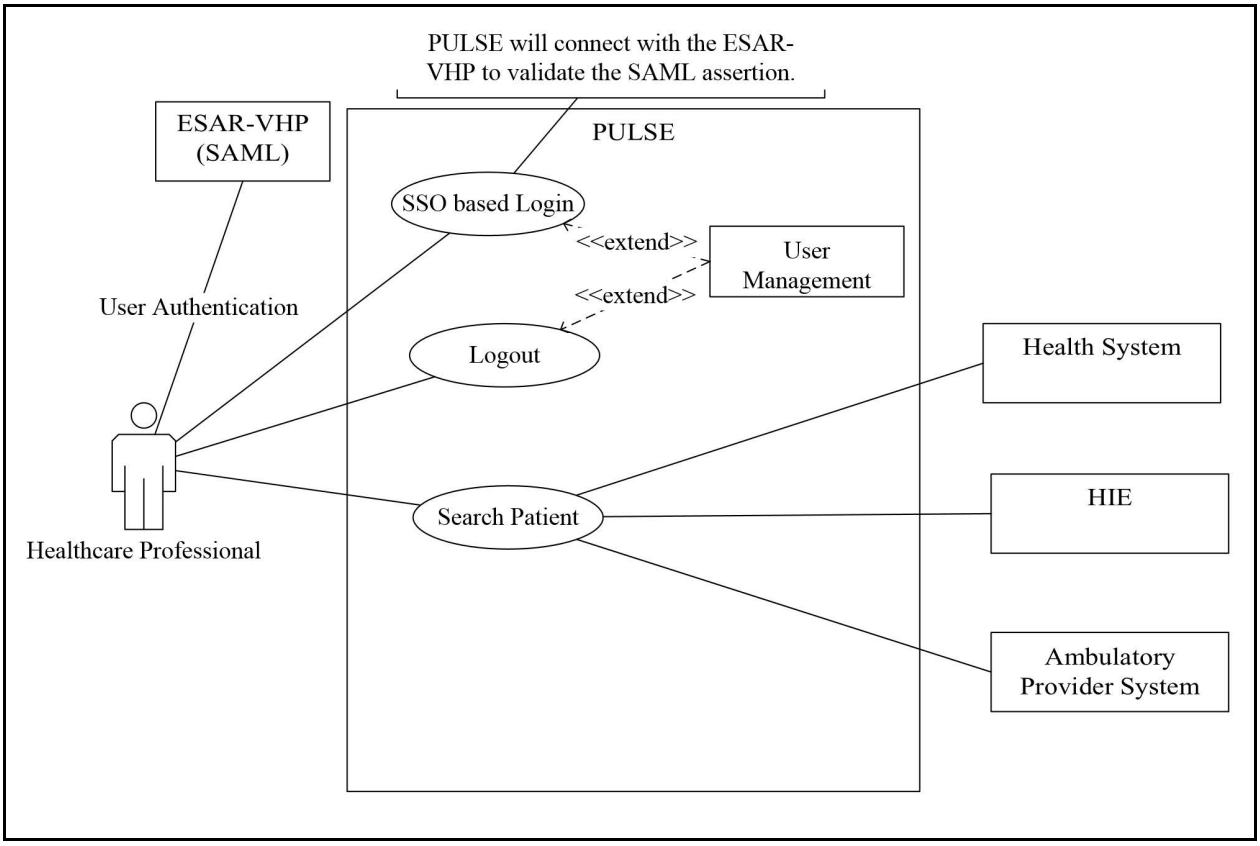


Figure 3: Direct PULSE Access

Use Case 2: External Health System User

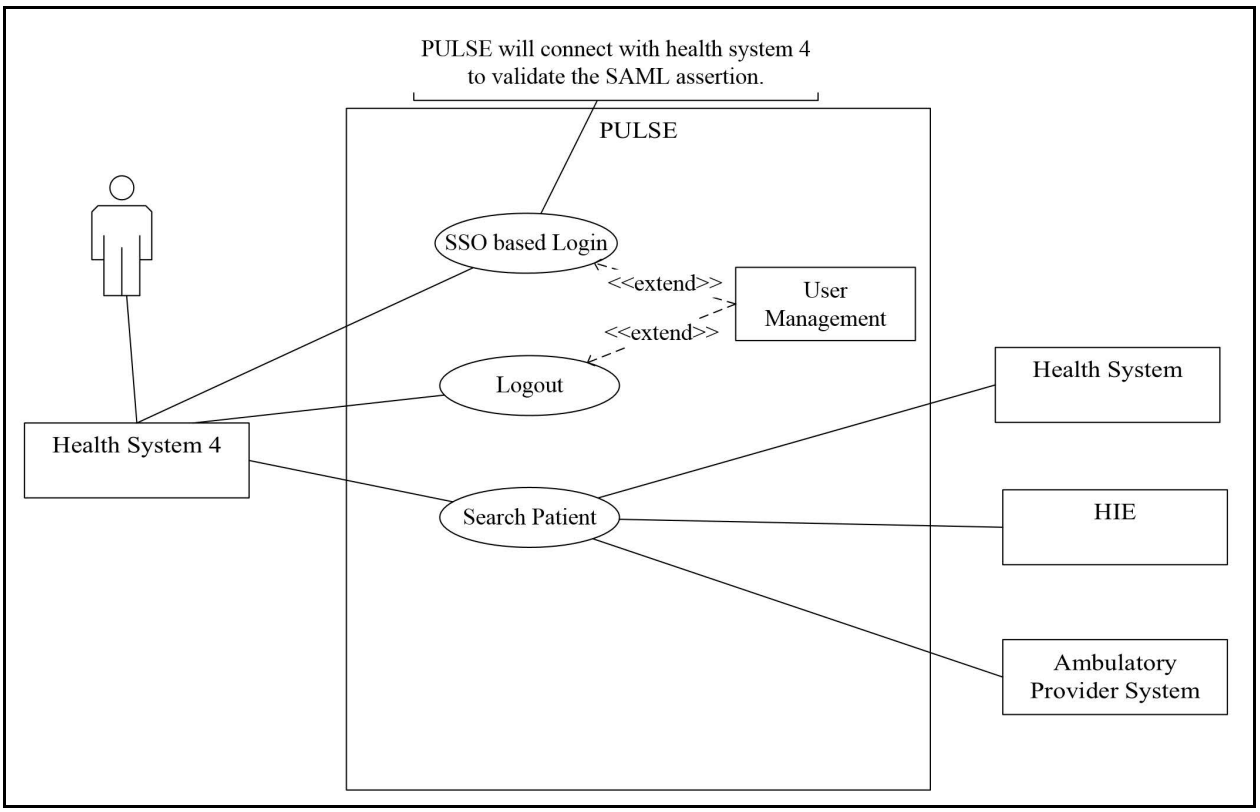


Figure 4: Indirect PULSE Access

Business Process Flow

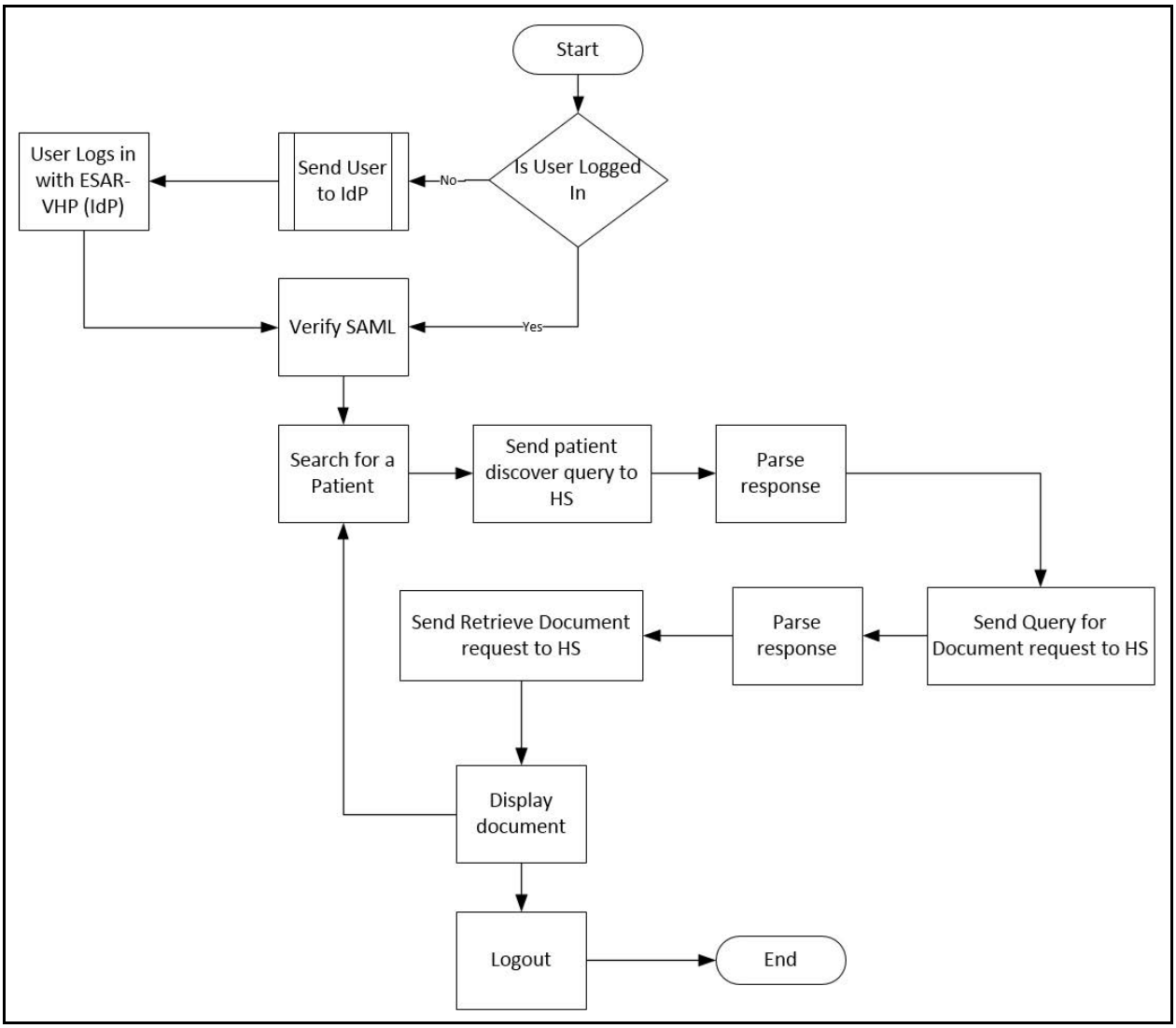


Figure 5: Process Flow

Application Architecture

This sub-section captures the application architecture of the PULSE system.

Application Architecture Principles

- System components must be designed in a service oriented fashion to provide maximum flexibility for the future.
- System components must be designed to use existing technical standards as much as possible, to promote interoperability and future extensibility.
- System components must be designed to handle a high volume of concurrent users.

- System components must be designed to provide acceptable response times for users.
- System components must be designed to support integration of existing and future health systems with minimal changes.

Logical Application Components

This view describes the logical application components and associated interactions.

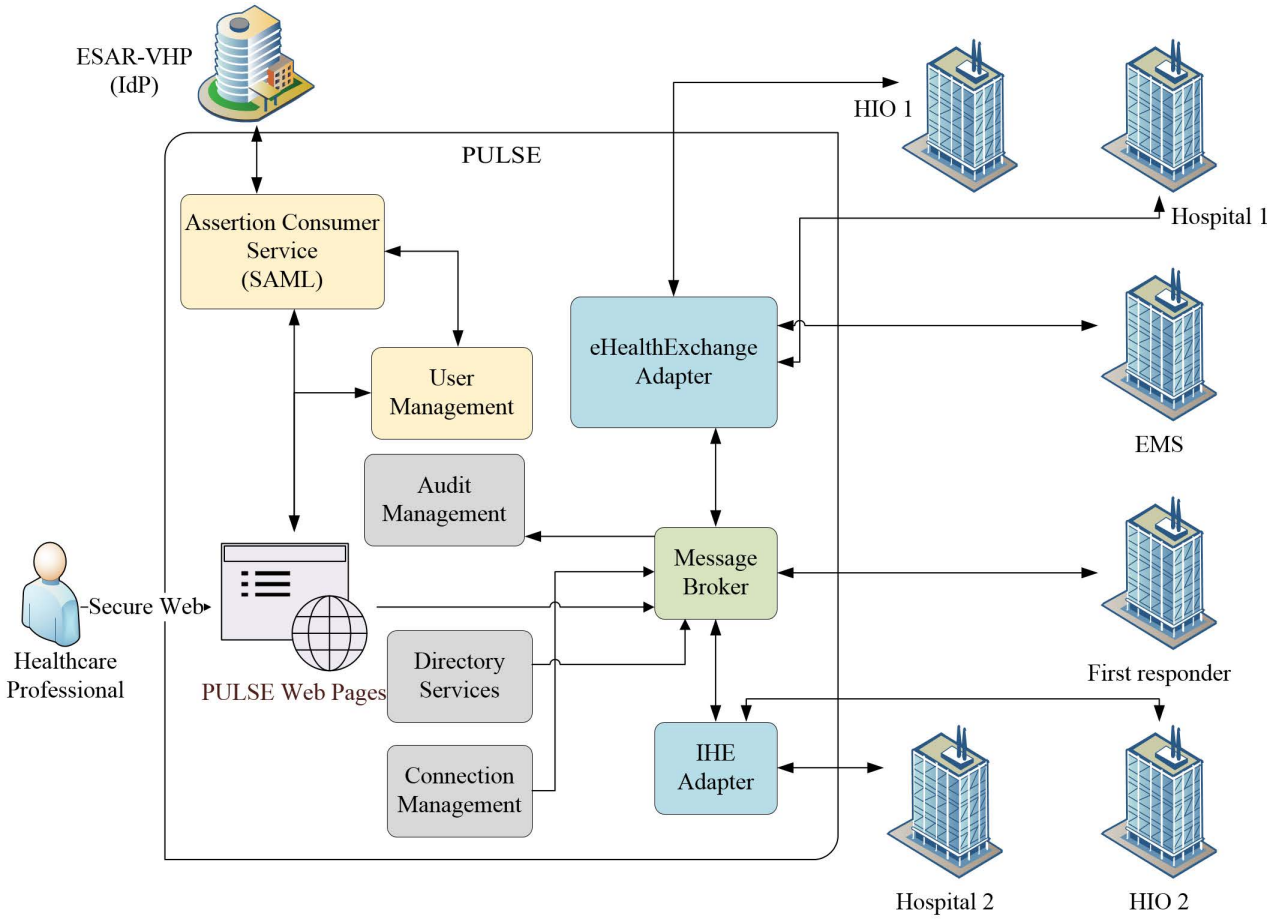


Figure 6: Logical Application Components

Process flows

This section describes the various workflows that can be supported by the PULSE system.

User Login

This diagram shows the process for user login through ESAR-VHP and the passing of the cred with privileges asserted to PULSE.

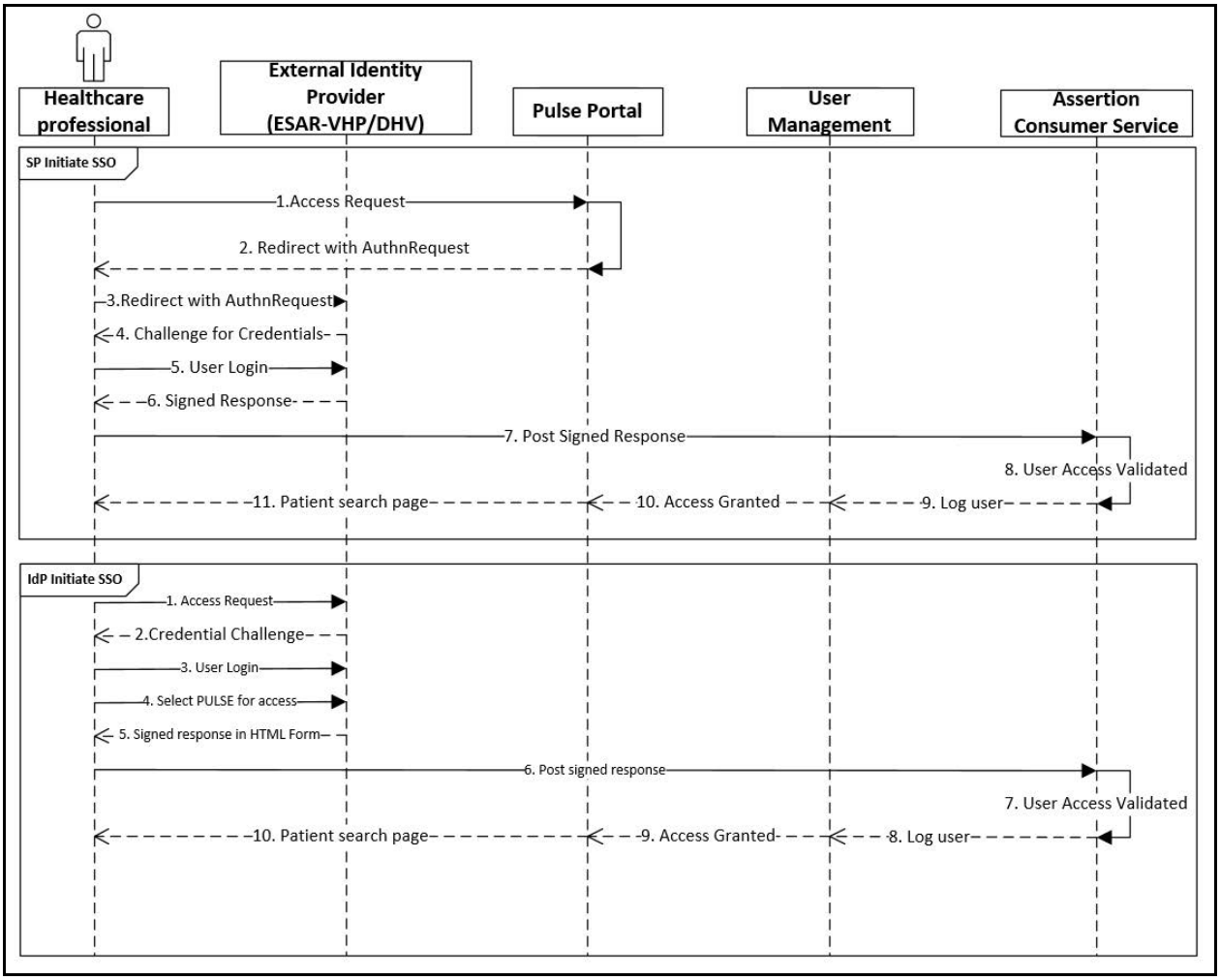


Figure 7: User Access Process

Service Provider (SP) Initiated SSO

1. User access PULSE Portal
2. PULSE redirects the user with AuthnRequest.
3. The browser processes the redirect and issues a request to ESAR-VHP single sign on service.

4. ESAR-VHP check if the user has an existing logon context, if not challenges the user for credentials.
5. User submits the credentials and IdP creates a logon context.
6. IdP builds a SAML response that includes the assertion. The response is included in the HTML form
7. Browser submits the form using "auto-submit" script, issues a HTTP POST request to send the form to the PULSE's Assertion Consumer Service
8. User access is validated.
9. Log user context in User management
10. User is granted access to PULSE
11. Patient search page displayed to user.

Identity Provider (IdP) Initiated SSO

1. User accesses ESAR-VHP .
2. ESAR-VHP checks if the user has an existing logon context, if not challenges the user for credentials.
3. User submits the credentials and IdP creates a logon context.
4. User selects PULSE access link in ESAR-VHP
5. IdP builds a SAML response that includes the assertion. The response is included in the HTML form
6. Browser submits the form using "auto-submit" script, issues a HTTP POST request to send the form to the PULSE's Assertion Consumer Service
7. User access is validated.
8. Log user context in User management
9. User is granted access to PULSE
10. Patient search page displayed to user.

IHE Participant

This view describes a PULSE user accessing a summary document of a patient from an IHE based health system.

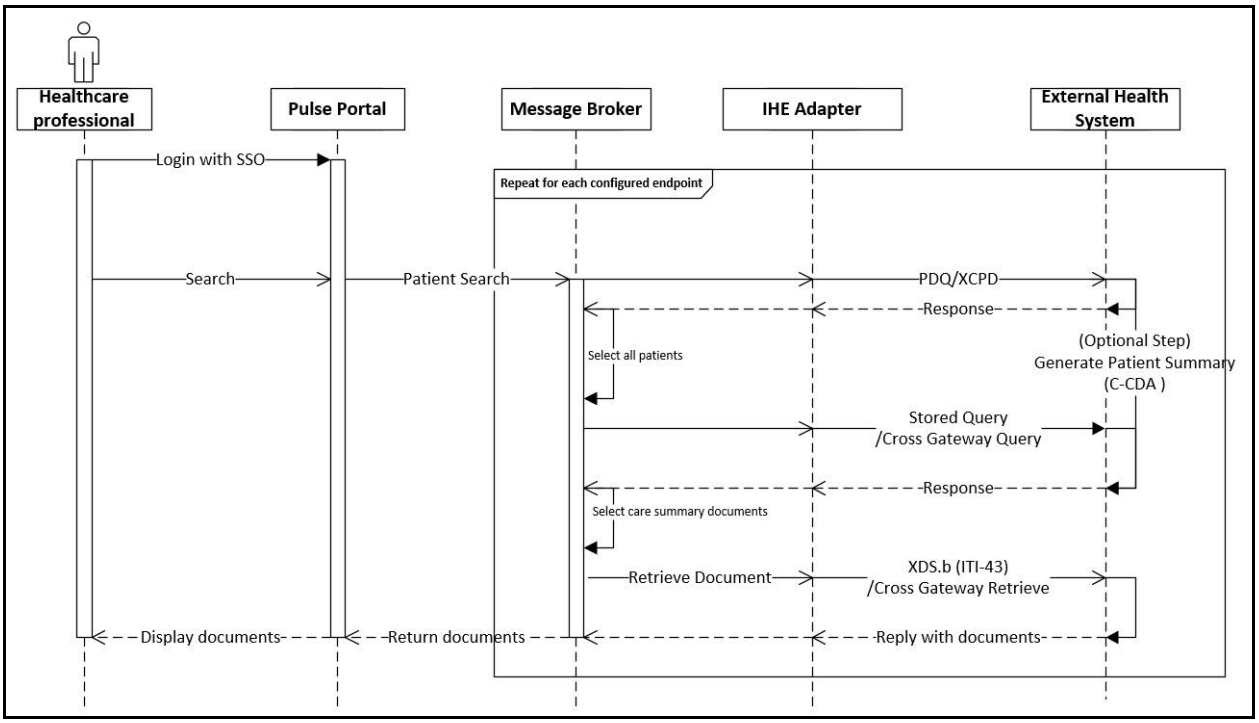


Figure 8: IHE Participant

1. User logs into PULSE through the 'User Login' process as defined in the previous section.
2. User searches for a patient using their demographic information (e.g. first name, last name, DOB, etc.)
3. Portal forwards the request to the Message Broker (MB) module.
4. MB forwards the request to the IHE Adapter.
5. IHE Adapter identifies the list of configured endpoints through directory Service to contact.
6. IHE Adapter constructs a PDQ/XCPD message and sends to the external health systems (HS) asynchronously with required and optional demographic data elements.
7. External system responds with either a single successive match or no unique match(s) found response. IHE Adapter forwards the response to MB.
8. MB provides the parsed data to IHE Adapter
9. IHE Adapter then constructs and sends Registry Stored Query or Cross Gateway Query to the external HS for a summary C-CDA.
10. External HS responds with a document ID.
11. This information is passed to the MB.
12. MB parses the response and issues a retrieve document request.

13. IHE adapter constructs the 'retrieve document' ITI-43/ Cross Gateway Retrieve message and send it to the external HS.
14. External HS responds back with the document which is forwarded the MB.
15. The document is forward by the MB to the portal, which then displays it.

eHealth Exchange Participant

This view describes a PULSE user accessing a summary document of a patient from an eHealth Exchange compliant health system.

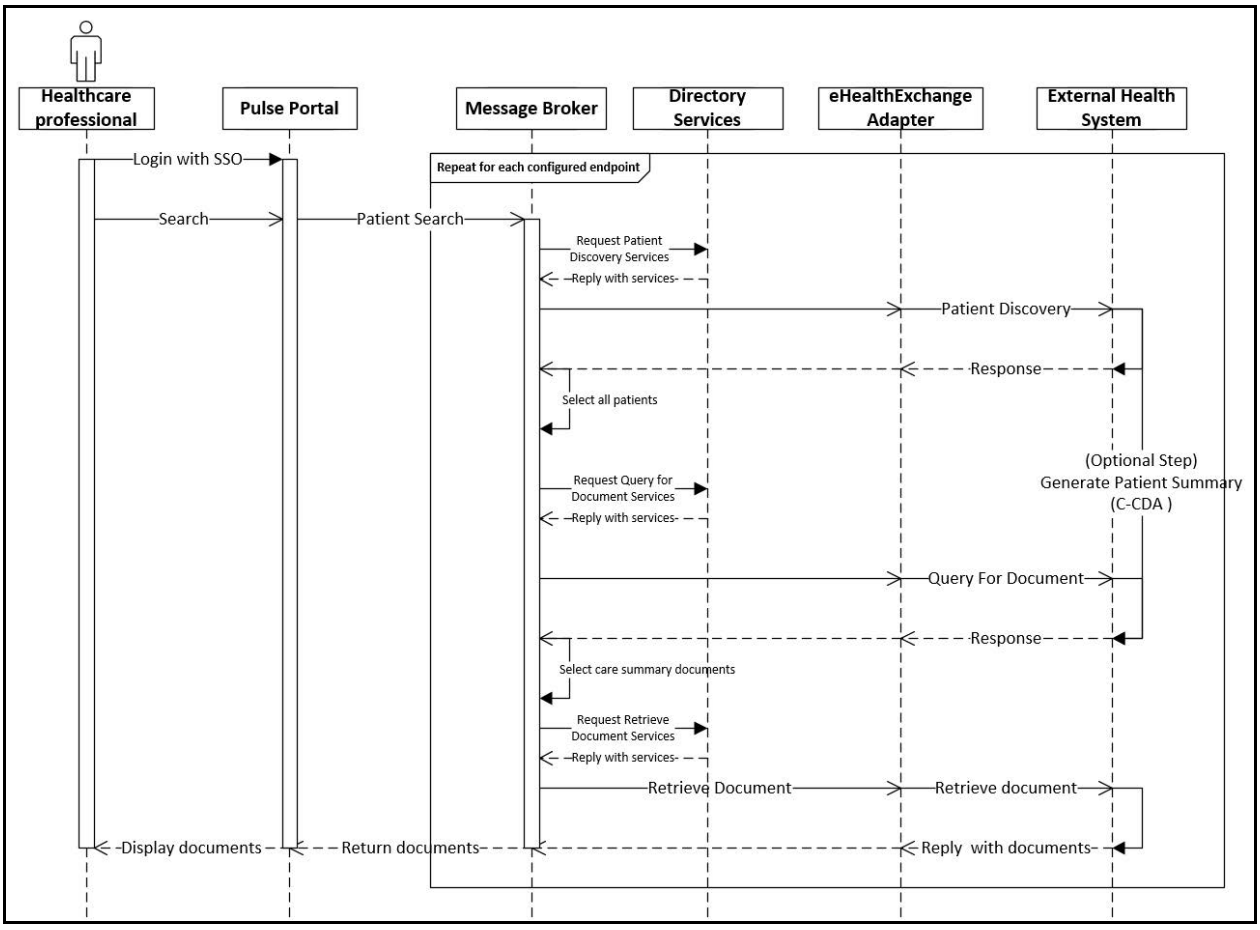


Figure 9: eHealthExchange Participant

1. User logs into PULSE through the 'User Login' process as defined in the previous section.
2. User searches for a patient using their demographic information (e.g. first name, last name, DOB, etc.)
3. Portal forwards the request to the Message Broker (MB) module.
4. MB queries the Directory service for Patient Discover endpoints
5. Directory Service responds with a list of services.
6. MB forwards the endpoint information and parameters to eHealth Exchange Adapter.

7. eHealth Exchange Adapter constructs a Patient Discovery message and sends to the external HS asynchronously.
8. External HS responds with either a single successive match or no unique match found response.
9. eHealth Exchange adapter forwards the response to MB
10. MB parses the response from the HS
11. MB queries Directory service for Query for Documents endpoints
12. Directory Service responds with a list of services.
13. MB forwards the endpoint information and parameters to eHealth Exchange Adapter.
14. eHealth Exchange Adapter constructs a Query for Document message for a summary C-CDA and sends to the external HS.
15. External HS responds with Document Id(s).
16. eHealth Exchange adapter forwards the response to MB
17. MB parses the response from the HS
18. MB queries Directory service for Retrieve Documents endpoints
19. Directory Service responds with a list of services.
20. MB forwards the endpoint information and parameters to eHealth Exchange Adapter.
21. eHealth Exchange Adapter constructs a Retrieve Document message and sends to the external HS.
22. External HS responds back with the document which is forwarded the MB.
23. The document is forward by the MB to portal, which then displays it to the user.

Physical Application Components

This view describes the physical application components and associated interactions.

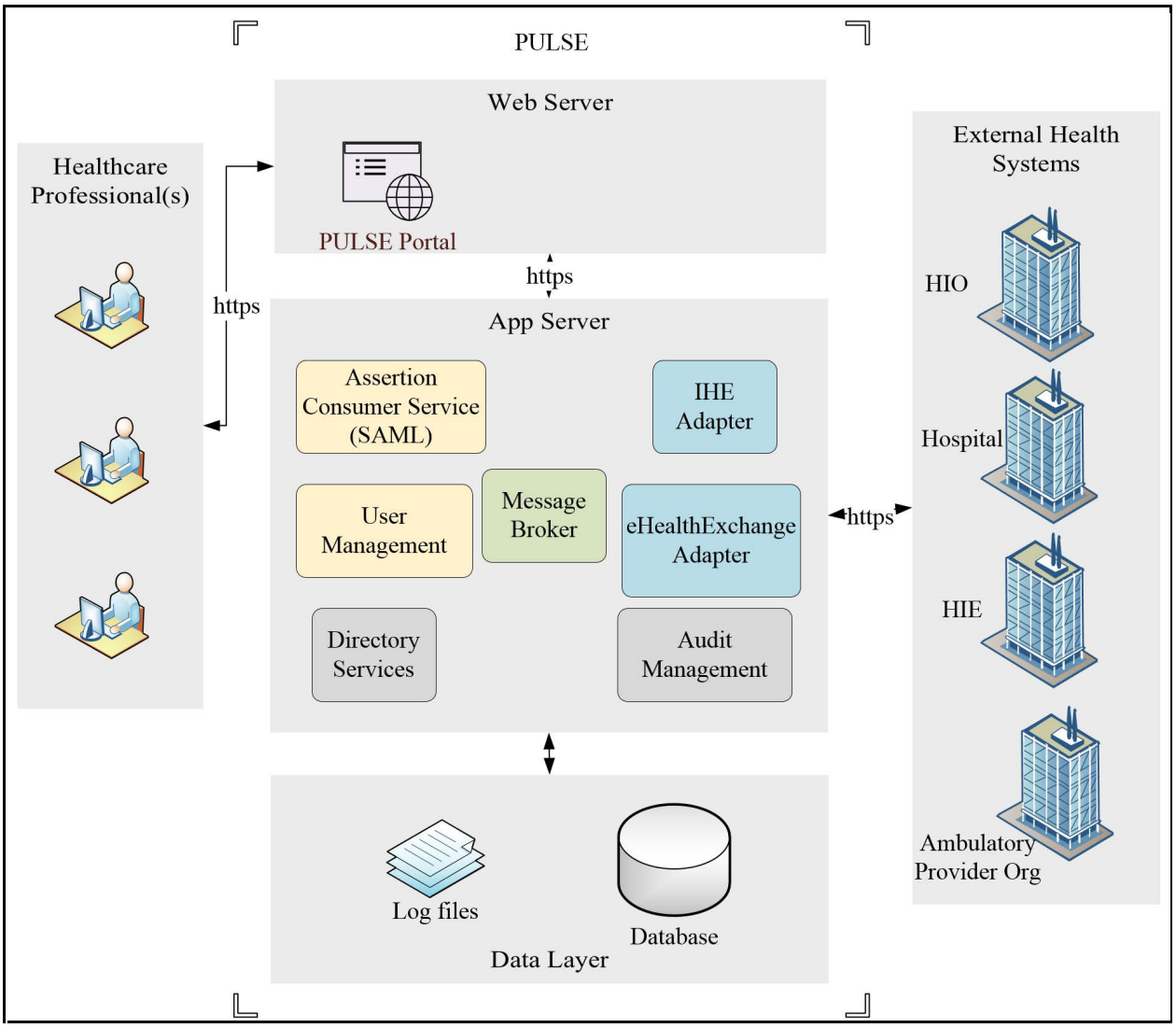


Figure 10: Physical Application Components

Technology Architecture

This section documents the technology architecture of the PULSE system.

Technology Architecture Principles

- Use Commercial Off the Shelf (COTS) products where they provide the required services.
- Select products based on vendor maturity to ensure long term sustainability of the product.
- Review product roadmaps before selection of any COTS components.

- Products and solutions implemented should have options for clustering for scalability and provide mechanisms for redundancy and automated failover.
- Solutions implemented should have mature change management and QA processes to ensure product updates are reliable and have good documentation for upgrades/rollback.
- Solutions implemented should minimize the number of network hops across the architecture layers to satisfy a single request.

System Architecture Components / Product Mapping

This section provides a mapping of the System Architecture Components and COTS products that can be used to implement the architecture. At this juncture, all of the architecture components are to be determined.

- PULSE web pages
- User management
- Assertion consumer service (SAML)
- Message broker
- eHealth Exchange adapter
- IHE adapter
- Audit management
- Connection management
- Directory service
- Database
- Operation system
- Web servers
- App servers
- Virtualization software
- Storage
- Firewalls
- Switches
- Certificates

Logical Deployment View

The Logical Deployment View for PULSE is shown below.

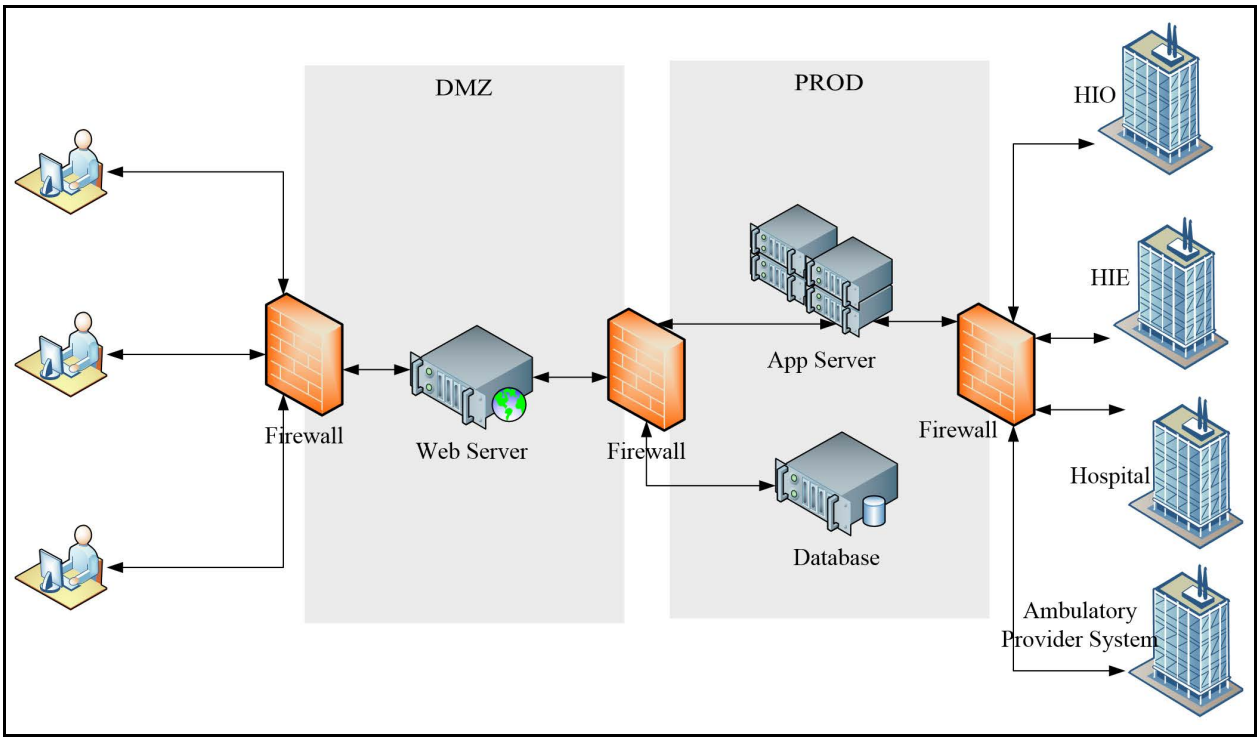


Figure 11: Logical Deployment View

Physical Deployment View

This section describes the physical deployment configuration of the PULSE system. The physical deployment view captures the physical hardware details.

Physical Server	Related Architecture Component	Configuration (OS/CPU/RAM)	COTS Products
TBD	TBD	TBD	TBD

Communication Protocols and Standards View

This table provides a list of all the protocols used in the various interactions between the various systems used internally and externally.

Protocols between External PULSE Components

Source System	Target System	Protocol/Standard	Target Ports	Purpose
Internet	Pulse Portal	https	443	Allow end users to access PULSE portal
Pulse	External Health Systems	https	443	Query for patient data

Protocols between Internal PULSE Components

Source System	Target System	Protocol/Standard	Ports	Purpose
Pulse Portal	User Management	https	443	Allow users to validate their access.
Pulse Portal	Message Broker	https	443	Allow users to search for patients
Message Broker	eHealthExchange Adapter	https	443	Send query parameters to adapter
Message Broker	IHE Adapter	https	443	Send query parameters to adapter
Message Broker	Directory Service	https	443	Query for service endpoints.
Message Broker	Database	tcp/ip	Unknown	Write audit information
User Management	Database	tcp/ip	Unknown	Read/write user account information

Security Architecture

This section documents the security architecture of the system. The security architecture identifies the various aspects of the architecture related to security and privacy. This document

only identifies the architecture components and does not identify the physical security controls and other aspects not related to the PULSE system such as change management.

Security Principles

- PULSE system must comply with state, federal and other applicable laws such as HIPAA.
- Solutions must not expose any of the sensitive patient level data to unauthorized users.
- Solutions should protect sensitive data, but disclose it when needed for delivery of care.
- Solutions must provide a way to determine system use and audit operations to ensure compliance with security controls.
- Solutions must plan for periodic security updates due to advisory notices issued from vendors, agencies and industry experts.

Network Segmentation

PULSE components are separated into logical network segments as described in logical deployment view. External users have access to the web pages hosted in the DMZ. These users do not have access to any application components or database residing in the PROD environment. The web pages access various application components via secure API calls. The application components interact with external systems using https.

Authentication, Authorization, and Access Controls for End Users

Authentication occurs within the ESAR-VHP application. An authorized user may select the PULSE portal application and when they do, their credentials and authorization levels are passed via SAML token to the PULSE application. All end-user registration, identification, and verification processes are managed through the State's ESAR-VHP program.

Encryption

At Rest

PULSE components do not store clinical information however transient PHI or metadata that can identify a patient or document may be stored as part of an audit record. Hence Log files and databases will be encrypted to prevent unauthorized exposure of PHI.

In Motion

All interaction between end users and PULSE is encrypted over TLS 1.2 protocol using a server side certificate. All interactions between PULSE and external systems are encrypted over TLS 1.2 protocol using server and client certificates. All certificates must use 2048-bit or higher encryption key.

System and Communications Protection

Communications between External systems and PULSE use encrypted communications (section 2.3.5). Communications between internal systems are also encrypted using appropriate secure

protocols. As part of implementation an access control process needs to be implemented for management of authorized access to PULSE infrastructure.

System and Information Integrity

The proposed architecture limits the surface area from which PHI could be exposed either accidently or maliciously.

Auditing

The audit management component of PULSE will track user activity. User Activity reporting may be included for enhancing the feature of PULSE. The audit system should also be capable of tracking MB-HS interactions for determination of responsiveness and conformance to SLAs.

Availability and Disaster Recovery

As PULSE is a system that is primarily meant to work during a disaster, a comprehensive DR plan for active PULSE components will need to developed and implemented as part of the PULSE implementation.

Technical Architecture Appendix

This section contains any general information that aids in understanding this document (e.g., background information, glossary, rationale).

References

- http://irb.ucsd.edu/cmia.pdf
- http://www.ca-hie.org/projects/cten/specifications
- California Data Use and Reciprocal Support Agreement (CalDURSA)
- Nationwide Health Information Network (NHIN) Patient Discovery Web Service Interface Specification
- Nationwide Health Information Network (NHIN) Query for Documents Web Service Interface Specification
- Nationwide Health Information Network (NHIN) Retrieve Documents Web Service Interface Specification
- Nationwide Health Information Network (NHIN) Web Services Registry Web Service Interface Specification
- http://www.ihe.net/Technical_Framework/upload/IHE_ITI_Suppl_XCPD.pdf
- http://ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol1.pdf
- http://www.hl7.org/implement/standards/index.cfm?ref=nav
- http://wiki.ihe.net/index.php?title=Profiles

Acronym Lists

The following acronyms are used in this document and in the referenced documents.

Acronym	Definition
CalDURSA	California Data Use and Reciprocal Support Agreement
C-CDA	Consolidated Clinical Document Architecture
CMIA	Confidentiality of Medical Information Act
COTS	Commercial-Off-The-Shelf
CTEN	California Trusted Exchange Network
DHV	Disaster Healthcare Volunteers – California's ESAR-VHP system
DR	Disaster recovery
ESAR-VHP	Emergency System for Advance Registration of Volunteer Health Professionals
HIPAA	Health Insurance Portability and Accountability Act
HL7	Health Level Seven which is a Standards Development Organization

Acronym	Definition
IdP	Identity Provider
IHE	Integrating the Healthcare Enterprise
PHI	Protected Health Information
SAML	Security Assertion Markup Language
SP	Service Provider
SSL	Secure Sockets Layer
SSO	Single Sign-on
TLS	Transport Layer Security
UDDI	Universal Discovery and Description Interface