PULSE

PULSE Community Edition

Getting Started Guide

Version 2.0 (Draft)

May 21, 2020

TABLE OF CONTENTS

Overview

The Patient Unified Lookup System for Emergencies – Community Edition, or PULSE Community, is a web portal that allows credentialed providers to find and view electronic patient data during disaster response. With a simple search on PULSE Community, credentialed providers can view documents that may include medications, allergies, diagnoses, and lab results for patients who are displaced outside of their normal health care environment.

There are two common use cases for which PULSE Community may be deployed. The first is to access clinical history of patients seeking medical treatment in alternate care facilities, for example in a shelter, quarantine site, or vaccination clinic. These settings typically lack access to a traditional electronic medical record (EMR) and providers may lack access to clinical data that is essential to timely and accurate patient care decisions. The second is in support of public health authorities who wish to access key clinical information to supplement patient demographics information, conduct clinical case augmentation, and perform epidemiological assessments. Though PULSE was originally designed for use after natural disasters such as hurricanes and wildfires, both use cases proved to be salient during the recent coronavirus (COVID-19) response.

Background

PULSE Community is the current evolution of the open-source PULSE technology platform. The first version of PULSE was developed in 2014 by Ai in partnership with the California Emergency Medical Services Authority (Cal EMSA) with funding from the Office of the National Coordinator for Health Information Technology (ONC), a division of the Department of Health and Human Services (HHS). Since then, Cal EMSA has successfully deployed the initial version of PULSE to assist in multiple wildfire responses. In 2018, The Sequoia Project, Inc, joined this partnership and now leads the PULSE Advisory Council. Comprised of nationwide representation from public health and emergency preparedness experts, this body has been instrumental in guiding the national-level rollout of PULSE and working closely with states on their planning processes. In 2019, HHS ONC committed additional funding to nationally scale PULSE's connectivity to the national health information networks. This federally supported version of PULSE is known as PULSE Community.

PULSE Community is intended to be scalable, flexible, and non-proprietary. Accordingly, the source code used to create PULSE Community will be publicly available on ONC's GitHub site in summer of 2020. Detailed technical documentation for PULSE administrators, including information on how to operate, configure, and maintain PULSE, will also be publicly available. Collectively, the detailed technical documentation and the *PULSE Community Getting Started Guide* will provide important foundational information to organizations or states who wish to build, implement, and deploy their own PULSE Community.

Importantly, the PULSE Community technology will be most successfully implemented and deployed as part of a comprehensive PULSE program. In addition to the technical architecture and source code of PULSE

Community, successful implementation and deployment of the overall PULSE program will require financial investment, human capital, policy alignment, integration with existing systems, connection to the national health information networks, IT security procedures, and ongoing testing and system maintenance. This *PULSE Community Getting Started Guide* will assist the reader in planning and executing a PULSE program by articulating the range of requirements to be considered.

Purpose of this Document

This *PULSE Community Getting Started Guide* will help State, local, and territorial and tribal agencies and their designated partners (i.e., Organizations)that would like to use the PULSE Community source code to build and implement the PULSE Community technology to better understand the programmatic, governance, policy, technology, and financial requirements that will contribute to success. Taken together, these requirements will lead to a comprehensive PULSE program that reaches beyond the technology.

The guide does not include source code for PULSE Community or the highly specific technical documentation that describes how to implement, operate, configure, or maintain PULSE Community. These documents will be available on ONC's GitHub site in summer of 2020.

Note: *As of the release date of this version of the PULSE Community Getting Started Guide, the PULSE Community technology is undergoing certain enhancements to improve its functionality and ease of use. As these enhancements are further developed and tested, some of the features and technical specifications include in this section may change. The final version of this document, which will be available later in 2020, will include all features and technical specifications related to these enhancements.*

The PULSE Community Technology vs. The PULSE Program

Jurisdictions that are concerned about the ability to care for patients during natural disasters (e.g., wildfires, floods, hurricanes, earthquakes, etc.), mass casualty incidents (e.g., mass shootings, train derailments, explosions, etc.), outbreaks or pandemics, or planned special events (e.g., large sporting events, political rallies, etc.) may wish to implement and deploy the PULSE Community technology and build a complementary PULSE program to support it.

The PULSE Community technology is a web-based tool that allows disaster health care volunteers to search for patient health and medication histories over national health information networks. Such access to patient health history can be critical for patients who have been displaced from their homes and routine care settings and are seeking assistance for acute or chronic conditions in shelters or other alternate care facilities (ACFs). PULSE Community is designed to connect to the eHealth Exchange. This enables query capabilities to 61 regional and state health information exchanges (HIEs), four Federal Agencies, 75 percent of U.S. hospitals, over 70,000 medical groups, and over 5,200 dialysis centers. Additionally, eHealth Exchange is now a Carequality implementer which additionally provides access over 600,000 care providers and the CommonWell network.

Successful implementation and deployment of the PULSE Community technology is highly dependent on several factors that are independent from the technology itself. For example, local, state, and federal laws regarding the safe and responsible exchange of protected health information must be followed. There should be a firm understanding of who is responsible for building, maintaining, securing, and updating the PULSE Community technology. Programmatic and technical costs must be budgeted for and executed against. The deployment and implementation of PULSE will be dependent on state disaster preparedness and response authorities, and may be contingent on local, state, or federal disaster declaration processes. The PULSE program is intended to ensure these and other programmatic, governance, policy, technology, and financial requirements are in place to support implementation and deployment of the PULSE Community technology.

An effective PULSE program can help Organizations:

1. Ensure that disaster health care volunteers have access to patient records when treating individuals who have been displaced by disaster;
2. Provide real-time electronic access to health and medication histories for disaster evacuees or individuals seeking care outside of routine care sites; and
3. Provide access to patient records that are maintained in national health information networks.

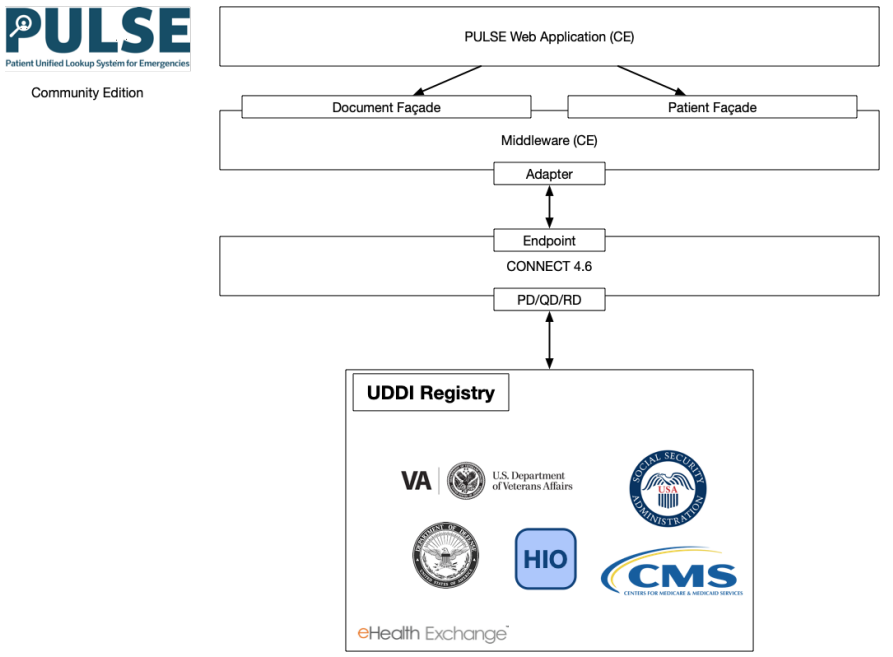
This document will help organizations better understand the requirements for both implementing and deploying the PULSE Community technology and for building a complementary PULSE program.

The PULSE Community Technology: Basic System Architecture

Using the PULSE Community code on the ONC GitHub site, it is possible for an organization to build their own version of a PULSE Community product. This section provides information regarding the basic system architecture that will be visible from outside the system as well as an explanation of the different ways users can interact with PULSE Community.

From a technical standpoint, PULSE Community is comprised of the user-facing web application, middleware, and back end CONNECT technology (Figure). A "user" (typically a disaster health care volunteer) will interact with PULSE Community securely over the Internet via a browser using a web-based portal application that is exposed by PULSE Community. Once logged in, the user is brought to a search screen that allows patient demographic data (e.g., name, address, date of birth, etc.) to be input and queried against across any of the connected national health information networks. Responding networks provide a list of documents that match the demographic information for the queried patient; that list appears as search results in PULSE Community. The user can then open and view the documents, which typically contain information about the patient's health history including diagnoses, medications, allergies, and immunizations.

Figure. PULSE Community Technology System Architecture



User Roles

PULSE Community is designed to allow access to certain features based on designated User Roles. No roles will have access to other roles' functions. However, a user may be assigned multiple roles, thereby gaining access to multiple functions.

The three user roles included in PULSE Community are:

1. **PULSE Administrator**: This user type can access all features and functions of PULSE Community. An Administrator can access administrative or configuration functions via authenticated access to underlying server systems and configuration files.
2. **Basic User**: This user type must be manually verified by the PULSE Administrator or through a single sign on connection from an existing provider authentication database and can access the system through a web browser to query for a patient, query for existing documents related to the matched patient, and retrieve documents relevant to the care and treatment of the patient by their regular health care providers.
3. **Auditor**: This user type can access only the reporting functions of the system. This role can be used alone or used in combination with other roles.

PULSE Community System Components

The PULSE Community web-based portal consists of three main functional components:

1. **PULSE User Interface (PULSE UI)** – PULSE Community enables appropriately verified disaster health care volunteers to access a patient's electronic clinical information during disasters. Users will access health information through a web-based portal and can search for and retrieve information from within connected electronic health record systems or health information exchange systems. The PULSE UI includes a Basic User Interface and an Administrator Interface, which can be thought of as the different "views" available to the Basic Users and the PULSE Administrator.

2. **PULSE Authentication & Authorization –** PULSE Community includes two options for authenticating and authorizing access to Basic Users. In the first option, Basic Users will login to PULSE Community via the main PULSE UI and are authenticated using Single Sign On (SSO) via Security Assertion Markup Language (SAML) to an external provider verification system such as a state's Emergency System for Advance Registration of Volunteer Health Professionals (ESAR-VHP). Additional integration points may be required depending on the organization's technology ecosystem. In the second option, organizations that do not wish to use SSO to an external provider verification system can manually populate appropriately authorized providers into the PULSE Community system through the Administrator Interface in the PULSE UI.

3. **National Network Connectivity** – The final functional component of the PULSE Community web-based portal is the UI that displays patient health information that has been obtained from data

sources through connection to national networks. PULSE Community currently supports an integration point to eHealth Exchange[1] which is now a Carequality[2] Implementer providing access to the CommonWell[3] network.

[1] https://ehealthexchange.org/
[2] https://carequality.org/
[3] https://www.commonwellalliance.org/

The PULSE Community Technology: Technical Requirements

This section describes the specific features and base technical requirements for the PULSE Community technology. The information included is intended to give implementers an overview of PULSE Community, the main components of the system (i.e., the PULSE User Interface (UI), PULSE Authentication & Authorization, and National Network Connectivity), and certain technical considerations that should be planned for if pursuing a PULSE vendor to build, implement, and deploy the PULSE Community technology.

Note: *As of the release date of this version of the PULSE Community Getting Started Guide, the PULSE Community technology is undergoing certain enhancements to improve its functionality and ease of use. As these enhancements are further developed and tested, some of the features and technical specifications include in this section may change. The final version of this document, which will be available later in 2020, will include all features and technical specifications related to these enhancements.*

PULSE User Interface (UI)

The PULSE UI includes a Basic User Interface and an Administrator Interface that together encompass the following functions to meet patient care requirements and administrative use cases and needs.

Basic UI Features

- SSO via SAML Community to an external provider verification system
- Ability to assign a user to an alternate care facility (ACF)
- A search function for patient matches based on an individual's demographic information
- Functionality to list and display available documents for a given patient match returned by data sources on the national network
- Retrieve documents, one at a time, from among the search results
- A patient document viewer for Consolidated Clinical Document Architecture (C-CDA) documents

Administrator Interface Features

The PULSE Community administrator requires an overarching view of the usage, logins, and metrics when the platform is deployed. The following features are included in the administrator interface:

- The capability for authenticated Administrators to activate and deactivate PULSE Community
- The ability to manually manage user access depending on the configuration with an external system
- The ability to create ACFs
- An administrator dashboard that includes basic user usage statistics, active ACF locations, number of active users, number of patient searches, and number of successful document retrievals

- Audit log capabilities to record information including emergency health information look up queries received, queries and requests placed to external systems, responses to those requests, and other activities

Required Technical Architecture for the Basic User and Administrator Interfaces

- PULSE Community is designed to leverage Amazon Web Services (AWS) infrastructure. This allows PULSE Community to be deployed in a scalable cloud hosted infrastructure leveraging multiple technologies[4] including:
  - Docker containers[5]
  - Various AWS databases and data stores including S3, Aurora, RDS
  - AWS Compute services including Lambda, EC2, and EKS
  - AWS Network & Content Delivery including VPC, Route 53, and Cloud Map
- PULSE Community is composed of several components. The underlying programming languages for different components are:
  - The UI and web application are based on JavaScript
  - The SSO and SAML portions are based on Java
  - The open source CONNECT is based on Java
  - The business logic of PULSE is based on .NET Core
- PULSE Community:
  - Supports the English language
  - Is available through a web browser and will scale to the size of the device screen
  - Is not a mobile application
  - Is not available in the Apple or Android application stores
  - Must run on a web browser that has been released in the past two years from a common vendor and supports Javascript and HTTPS
  - Requires HTTPS and TLS security infrastructure using X.509 certificates

PULSE Authentication & Authorization

When PULSE Community is activated, the web portal is opened and easily accessible through a URL. PULSE Community includes two options for authenticating and authorizing access to Basic Users. In the first option, Basic Users will login to PULSE Community via the main PULSE UI and are authenticated using SSO to an external provider verification system - a state's Emergency System for Advance Registration of Volunteer Health Professionals (ESAR-VHP). In the second option, organizations that do not wish to use SSO to an external provider verification system can manually populate appropriately authorized providers into the PULSE Community system through the Administrator Interface in the PULSE UI.

[4] https://aws.amazon.com/products/
[5] https://docs.aws.amazon.com/AmazonECS/latest/userguide/docker-basics.html

Authentication & Authorization by SSO

To use PULSE Community in tandem with an existing external provider verification system, the following are required:

- Integration and secured network connectivity with the external provider verification system portal through SSO
    - Ability to facilitate interactions with other components using SSO and secure industry SAML Community standards to identify and authenticate appropriate end users

Required Technical Architecture

- PULSE Community:
    - Allows SSO users to login to the PULSE application
    - Can integrate with any ESAR-VHP application that supports SSO with SAML Community from a supported browser
    - Must run on a web browser that has been released in the past two years from a common vendor and supports Javascript and HTTPS

National Network Connectivity

National network connectivity enables PULSE Community users to query the national networks for health information that will be presented in the UI. PULSE Community is designed to connect to eHealth Exchange, which now also connects to Carequality and CommonWell.

Overall System Requirements

National Network Connectivity Features

- A query function that links to external data sources (one query at a time) using interfaces to identified national and potentially regional systems
- Queries external data source(s) for documents containing health information for a matched patient identified through Patient Discovery
- Retrieves documents containing health information for the matched patient from external data sources using a standards-based web service that allows PULSE to retrieve specific documents through Query for Documents and then Retrieve Documents transactions.
- Provides the ability for the PULSE Directory Service to connect to the eHealth Exchange nationwide network Directory Service. Future versions of PULSE may consider enhanced directory capabilities to include other directories (for example, Care Quality), but this functionality is not included at this time.
- Connects to eHealth Exchange

Notes:

- Other networks including Carequality, CommonWell, and custom or regional networks may be available in the future
- This functionality requires an appropriate directory of external health care systems using the Universal Description, Discovery and Integration (UDDI) specification

Transport Standards

Using IHE standards, the PULSE system connects a national network such as eHealth Exchange, health systems, or health information organizations as an interoperability broker to query for patients, return lists of documents for a given patient, and then retrieve and display a C-CDA document. The specific IHE transactions used are: Cross-Community Patient Discovery (XCPD), Cross Gateway Query, and Cross-Community Gateway Retrieve, respectively.

- **Patient Discovery:** PULSE can search for a patient via at least one node or organization on the eHealth Exchange or similar network. The specific IHE profile used is ITI-55: Cross-Community Patient Discovery (XCPD)
- **Query for Documents:** PULSE can return a list of documents for a single patient from at least one node or organization on the eHealth Exchange or similar network. The specific IHE profile used is ITI-38: Cross Gateway Query, which is modeled after the Registry Stored Query ITI-18 transaction
- **Retrieve Documents:** PULSE can return a full document for a single patient from at least one node or organization on the eHealth Exchange or similar network. The specific IHE profile used is ITI-39: Cross Gateway Retrieve, which is modeled after the Retrieve Document Set ITI-43 transaction
- **Viewable Documents:** PULSE can display both 1.1 and 2.1 C-CDA documents. Since PULSE will be used during emergencies to provide immediate treatment to patients it is believed that a summary of care in the C-CDA format would be helpful as hospitals and providers produce these documents for their transitions of care and encounters. C-CDAs commonly contain demographics, problems, medications, and allergies.

Required Technical Architecture

- IHE Technical Framework integration profiles[6]
- Health Exchange network standards and requirements
- HL7 Consolidated Clinical Document Architecture (C-CDAs)
- Carequality Connected Agreement (CAA), approved 5 November 2015
- Carequality Query-Based Document Exchange Implementation Guide Version 1.0, adopted 5 November 2015
- HL7 CDA Release 2, CCD.
- HITSP Summary Documents Using HL7 CCD Component HITSP/C32
- HL7 FHIR® Standard for Trial Use 3 (STU3), when released1
- IHE IT Infrastructure Technical Framework Volume 2a (ITI TF-2a) Transactions Part A Revision 13.0, released 9 September 2016

[6] https://www.ihe.net/resources/technical_frameworks/#IT

- Nationwide Health Information Network Messaging Platform Specification Version 3.0, released 27 July 2011
- Nationwide Health Information Network (NHIN) Authorization Framework Specification Version 3.0, released 27 July 2011
- Nationwide Health Information Network (NHIN) Patient Discovery Web Service Interface Specification Version Community, released 27 July 2011
- Standards-based SOAP web service that allows PULSE to retrieve specific documents identified through Query for Documents containing health information specific patients identified

The PULSE Community Technology: Additional Implementation Considerations

Testing and Certification

PULSE Community must undergo the formal eHealth Exchange testing program[7] that validates the compliance of the PULSE Community technology with the eHealth Exchange Performance and Service Specifications and allow for standardized interfacing into other common networks. This testing program has several components including security, content, and network connectivity testing. The governance process of the PULSE Program will need to manage the non-trivial application, testing, and connectivity processes required to join, participate in, and connect with eHealth Exchange.

Security

PULSE Community implementers (i.e., entities that deploy and host PULSE Community) should use a minimum of two forms of security to ensure confidentiality, authenticity, and integrity of sensitive information managed by the system. With that, any infrastructure as code (IaC)/keys/secrets/configuration will not be included in the source repository and potential technology vendors should demonstrate how they can manage that information privately in an existing system or use external systems for security functions (e.g., AWS OpWorks).

Questions to ask a PULSE Community implementer can include, but are not limited to:

1. Has your engineering process has been accredited by HITRUST?
2. How do you isolate networks to reduce our risk surface (e.g., separation of DMZ, application, and durable data store subnets)?
3. How do you utilize end-to-end encryption in transit?
4. How do you ensure all durable data stores are encrypted at rest?
5. How do you practice least privilege access (e.g., deny all, allow explicit)?
6. How do you perform quarterly penetration tests with an independent third party?
7. How do you offer security guidance and recommendations to the state resources securing state-specific implementations and integration points?
8. How do you follow the state and federal privacy laws, including Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the consent requirements of national networks?
9. How do you procure and provision browser (and backend) certificates with proper security?

While these are a subset of proper questions to ask, much of the security infrastructure will be dependent upon a PULSE Community implementer's operational services and capabilities. The security requirements should also be in line with any federal, state, and local security requirements, as well as the security requirements of any system integrated with PULSE Community. This may include the external provider verification system or existing health information exchange networks.

[7] https://ehealthexchange.org/testing-program/

The security requirements to participate with eHealth exchange are posted as part of their Testing Program.

System Redundancy

A major technical consideration is the location where PULSE Community components, specifically the interoperability broker and the user web interface, are hosted. Both items should implement a disaster recovery server or location that is in a separate geography from the main infrastructure. This ensures that in the event of a disaster in the location where the interoperability broker and web interface are hosted, PULSE Community will have a fail over server and continue to be available. Similarly, health systems and health information exchanges have their own disaster recovery plans, which typically include a second fail over environment and servers. For PULSE Community to have access to their data during a disaster, health systems and health information exchanges may need to build two connections to the interoperability broker, one for their primary servers and one for their disaster recovery servers.

The PULSE Program: Basic Requirements

As mentioned, successful implementation of the PULSE Community technology will require a comprehensive PULSE program that ensures programmatic, governance, financial, and technical requirements are met.
Jurisdictions that wish to build, implement, and deploy a PULSE program should include a wide variety of stakeholders from across state and local government who may be involved in PULSE deployment (e.g., Emergency Management, Medicaid, Public Health, etc.) in the planning process. The following basic programmatic requirements should be considered:

Administrative Leadership

- Identify a leader(s) to champion and advocate for successful implementation of PULSE
- Identify all stakeholders required for the successful implementation of PULSE
- Establish accountability for the PULSE program from among stakeholders and partners
- Ensure that state and local disaster response leaders support the PULSE program

Human Resources

The successful PULSE program will leverage personnel with program management, IT, financial, and policy experience. The following are potential roles for personnel who contribute to the PULSE program. Governance of the PULSE program is vital to these roles:

Activation Authority

The Activation Authority is the person or entity with the legal or political authority to authorize the activation and use of PULSE in the jurisdiction during declared disasters or public health emergencies.

Executive Sponsor

The Executive Sponsor will direct the successful implementation of the PULSE program and be responsible for overseeing funding and contracting, program implementation, maintenance, and deployment, and abidance by federal, state, and local laws and policies. The Executive Sponsor will also facilitate the relationship between the funding and implementing organizations and work closely with the PULSE Administrator to oversee use of the PULSE platform during disasters.

PULSE Administrator

The Administrator will be responsible for activating, maintaining, and deactivating the PULSE Community platform during an emergency. The Administrator has access to all features and functions of PULSE Community and can use the configuration functions within the system to customize the user experience. The Administrator is responsible for facilitating user access to

PULSE, whether through a SSO function to an existing volunteer database or through manual entry of volunteers into the system.

Basic Users

The Basic Users will typically be a disaster health care volunteer. Basic users can access the PULSE Community platform through a web browser to query for patient matches, query for existing documents related to the matched patient, and retrieve documents relevant to the care and treatment of the patient.

Support Personnel

Identify qualified information technology and emergency preparedness personnel to support the implementation and deployment of PULSE Community.

Questions to Consider:

- Within the jurisdiction's incident command structure, who has authority to declare a disaster or public health emergency? Who has the authority to deploy state resources?
- Which state agencies typically lead and support shelter staffing operations during disasters?
- Who will decide to activate and deploy the PULSE Community technology during a disaster?
- What are the triggers for PULSE Community activation?
- What information is needed to support the decision to activate PULSE Community?
- Who will be responsible for communicating about PULSE Community activation and ongoing operations during a disaster?
- Do you have an existing source of Basic Users/disaster health care volunteers?
- Who is responsible for training Basic Users/disaster health care volunteers to appropriately utilize PULSE?
- Who is responsible for ongoing technical and programmatic support for PULSE?
- When will PULSE Community be deactivated?
- What deactivation procedures are necessary?

Governance

Jurisdictional governance of the PULSE program will vary depending upon several factors, such as whether PULSE Community is implemented statewide or if implemented to address city, county or local needs. At a minimum, the jurisdiction will:

- Govern policies and oversee the operation of PULSE Community for jurisdiction events
- Determine who can access PULSE Community
- Define and decide when to activate, deploy and deactivate PULSE Community

- Integrate PULSE Community into existing disaster response plans and processes
- Coordinate with authorities and responders within the jurisdiction and with the PULSE Community administrator before, during, and after events

Governance of the PULSE program may be supported by liaisons from the organizations responsible for operating the PULSE Community technology platform, those with the authority to deploy state assets during disaster response, and those funding the program. These liaisons should have real-time communication with the Executive Sponsor and PULSE Administrator before, during and after an event. Establishment of a PULSE program governance body is recommended.

Support Services

PULSE Community deployment assumes that ACFs have been established and staff, equipment, and supplies are available. Appropriate staff and volunteer training must take place for proper use of PULSE. Deployment is also dependent upon ongoing access to the Internet and functioning IT infrastructure, as well as functioning connections to the health information networks. PULSE deployment planning should include considerations for ongoing program support and maintenance for these services.

- Develop a user guide that addresses operational issues occurring with the PULSE Community technology in the field for time- critical problem resolution.
- Define a change management process, in consultation with the governance body and PULSE administrator.
- Determine how change requests should be submitted, to whom and how they are prioritized and addressed.

State and Local Health Information Exchange Capacity

- Understand what health information exchange infrastructure and capabilities are currently available in the state or jurisdiction
- Identify whether other vendor-supported technologies that exchange health records for coordinated patient care are already in use
- Determine the proportion of the population that is included in local and state health information exchanges (the HIE may be able to provide this information) and whether these HIEs are participants of the national networks (eHealth Exchange, Carequality, Commonwell, etc.).
- Decide which regional, state, or national networks can provide the best coverage of the jurisdiction

Legal and Policy Considerations

Jurisdictions should develop policies and procedures to support PULSE programmatic, technical, and operational decisions. Policies may cover the following topics:

1. **Activation, Deployment, and Deactivation**
   - Identify the response scenario(s) for which PULSE Community is intended to be used. Define appropriate terms regarding the activation, deployment and deactivation of PULSE, particularly as related to acceptable uses under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and other applicable laws and regulations and as defined in any applicable data use agreements.
     - For which scenarios will PULSE Community be activated and available for use?
     - Will PULSE Community be used only during declared disasters or for other scenarios as well?
     - Who will be granted access to PULSE Community?
     - When is PULSE Community deactivated?
     - How will activation and deactivation be communicated?
   - Factors to consider include:
     - Type of event: Is this event likely to result in large numbers of ill or injured that would require activation of alternate care facilities or result in large numbers of people being evacuated from their homes and current medical support network
     - Expected duration of the event: The longer an event lasts, the greater the impact on normal health care services and the ability of patients to access those services
     - Number of people affected and how they are affected: What is the projected impact of the event? Do you expect many people effected, but not severely; or a smaller number of people affected dramatically?
     - Location (major metropolitan area vs. isolated area): If the event impacts a major metropolitan area then the number of people affected may be higher but there may be more available health care infrastructure. Isolated areas may have fewer health care resources so even a small number of casualties can require support.
     - Magnitude of event: Assess whether the event is serious enough to require activation of alternate care locations. PULSE enables health care providers who are not part of the local health care delivery system to access information about patients and more effectively triage and treat them. Not every event, even large-scale events, will create a demand for this service.

2. **Deployment Sites (ACFs)**
   - Determine whether PULSE Community will be available in all ACFs or limited to specific

locations
- Verify that the selected sites have the required technical capabilities (e.g., Internet, computers) and the Administrator and Basic Users can use and access them
- Identify the process by which ACFs may request PULSE Community implementation and deployment

3. **Access**
   - Identify requirements for access to PULSE Community (e.g., based on role, experience, training, etc.)
   - Determine whether a small group of licensed professionals will be pre-identified to train on and deploy PULSE Community
   - Decide whether unlicensed volunteers will be provided access to use PULSE Community (e.g., to serve as registrars at the ACFs)

4. **User Identity Verification**
   - Define how disaster health care volunteers granted access to PULSE Community
   - Identify the most appropriate data source for authenticating disaster health care volunteers (e.g., a state ESAR-VHP system)
   - Determine whether single sign on to PULSE Community (e.g., using the ESAR-VHP process) is required or if manual entry is preferred
   - Determine whether other means of identity verification of users will be required

5. **Patient Identity Verification**
   - Determine whether patients will be required to present identification to be queried
   - Determine the minimum demographic information (e.g., name, sex, date of birth, address, etc.) that will be required to perform a query
   - Identify whether there are special provisions for minors

6. **Training**
   - Identify whether training on PULSE will be required before access is granted
   - Determine the required frequency of training
   - Determine whether just-in-time training will be offered
   - Identify which elements of training are required to meet PULSE program goals, for example:
     - PULSE Community implementation procedure
     - HIPAA laws
     - Incident Command System
     - Privacy and Security

7. **Privacy and Security**
    - Determine how long search history and retrieved documents will be accessible
    - Determine whether users will be locked out if idle
    - Determine password and username complexity rules
    - Determine role-based control options
        i. For details regarding the user and group management functions and the roles defined for PULSE users, see https://github.com/Jasig/NotificationPortlet

8. **Alignment with Existing Programs**
    - Determine whether existing emergency preparedness programs or applications will require modification if PULSE Community is deployed
    - Identify whether PULSE Community may need to be customized to align with or complement other existing programs or applications that are used during a disaster response

9. **Alignment with Federal, State, and Local Laws**
    - Identify all federal, state, and local laws that govern access to protected health information during emergencies and disasters
    - Understand the implications of federal, state, and local laws on the PULSE Community program
    - Consider whether there are special requirements for certain populations (e.g., minors) or for access to record types (e.g., use of controlled substances)
    - Align with appropriate National Network requirements including, but not limited to the DURSA.
10. **Alignment with Data Use Agreements**
    - Consider all data use agreements that must be in place prior to PULSE deployment, for example as related to data exchange over the national health information exchange networks

Maintenance

Identify Exchange Connectivity

Ongoing connection to national health information exchange networks is required.

Ongoing Support, Maintenance and Performance Improvement

Periodic Testing and Drills

PULSE Community is expected to be idle for periods of time, until the system is activated and deployed for an event or disaster. It may be very challenging to find licensed professionals who are available during the disaster to test the PULSE Community platform. If unlicensed professionals are not

authorized users, it further limits the ability to test the platform during a disaster. It is critical that PULSE be tested periodically to have assurance of system readiness and availability. This can be accomplished through ongoing technical testing and table-top drills.

Test System Readiness and Availability

- Define process and frequency for ongoing testing to assure system readiness. This could include quarterly or biannual end-to-end testing or periodic technical testing to verify system uptime and availability.

Table-Top Exercises

- Develop and facilitate tabletop exercises, with end user engagement, to address:
  - Hypothetical scenarios
  - Scenarios in an environment with real patients
  - Assess whether the exercises (which typically use fictitious data) will use a test PULSE Community environment or a live PULSE Community environment
    - If a test environment is used for the exercise, it will be important to assess substantive differences from how PULSE Community would work in a live environment

Performance Improvement

- Determine who should be involved in periodic evaluations of PULSE Community to assess its performance and value in supporting disaster response efforts.
- Incorporate PULSE Community into existing performance evaluation processes and after-action reports to critique and improve disaster preparedness and response.

Communications and Information Management

- **Response Communications:** Determine who is accountable for a communications plan that incorporates PULSE Community into disaster response plans and communications.
  - Consider communications channels, protocols and approvals in coordination with other agencies, command center and Disaster Health Care Volunteer Coordinators
  - Establish clearly understood communications during an event that links to Incident Command
  - Provide disaster health care volunteers with necessary communication gear to support stable and secure communication. Plan for cell service to be unreliable.
  - Implement HIPAA-compliant physical, administrative and technical safeguards to protect the privacy and security of patient information, including authorized access to PULSE.

- **Awareness, Education and Outreach:**
  - Develop a communications package for PULSE Community.
  - Build awareness of the PULSE program and its role in disaster response efforts, among leadership, disaster response stakeholders and the user community.

Training

- **Prepare PULSE Training Materials**
  - Develop a PULSE Community Users Guide and rollout plan
  - Develop a PULSE Community training toolkit for disaster health care volunteers and administrators

- **Train End Users, Volunteer Coordinators and Administrators**
  - Deliver advanced and onsite training for local Disaster Health Care Volunteer Coordinators and volunteers on how to use PULSE Community
  - Define processes for technical support in coordination with the PULSE administrator

Funding Requirements

The cost to cover the technical implementation and ongoing operation of the PULSE program will vary depending upon jurisdictional decisions regarding construction, management, and administration of the system, whether a third-party vendor will operate or manage any aspect of the program, and any requirements or restrictions of the pursued funding sources.

Potential operating and technical costs that should be considered for a successful PULSE program include:

Operating Costs

- Physical equipment (e.g., laptops, Internet routers, power cables, printers, etc.)
- Supplies
- Site preparation
- Communications and outreach
- Education and training program and just-in-time training materials
- Program management personnel
- Information technology (IT) personnel

Technical Costs

- Certificates and web hosting
- Testing and participation fees for national health information networks
- System design and customization
- System maintenance
- IT security

Federal Funding Sources

The Federal Government offers several potential funding options for states that can help offset implementation, maintenance, and operation of the PULSE program. Many of these sources require a funding "match" that should also be considered when budgeting. Each of these programs also has different requirements that may result in necessary changes to the conceptualization of the PULSE program and/or the PULSE Community technology. This is not an exhaustive list of potential federal funding sources, and organizations should consult grants.gov and other publicly available resources for additional options.

Federal Financial Participation for HIT and HIE

The Centers for Medicare & Medicaid Services (CMS) offers federal funding at 90 percent matching rate for state expenditures on activities to promote health information exchange (HIE).[8] Federal Funding Participation (FFP) funding requests are submitted from State Medicaid Agencies to CMS and other federal agencies through the Implementation Advance Planning Document (IAPD) process. States must secure 10 percent of the funding amount to receive the 90 percent matching rate (90-10). Potential sources for matching funds include:

- State general funds to support emergency preparedness, public health, and/or Medicaid
- State dollars appropriated for health information technology infrastructure
- State tax on health care services
- State tax on commercial health insurance products
- Payor taxes/surcharges
- Vaccine trust account
- In-kind contributions, however state-supported staff time is not allowed

State Medicaid Agencies can pursue either 90/10 Health Information Technology (HITECH) administrative funding or the Medicaid Enterprise Systems (MES) IAPD. Each is discussed further below.

HITECH Administrative Funding- The HITECH Act provides funding for state administrative activities related to the development of core HIE services (e.g., designing and developing a provider directory, privacy and security applications, and/or data warehouses), public health infrastructure, electronic Clinical Quality Measurement (eCQM) infrastructure, and provider on-boarding. It does not provide funding for operations and maintenance costs or for any activities that do not directly support the Medicaid EHR Incentive Program. Below are some items to consider when pursuing HITECH funding:

- HITECH funds are only available until September 2021 for design, development, and implementation (DDI) uses
- HITECH funds are available for standing up a new system, tool, or program but are not to be used for ongoing maintenance
- Requests for funds through the IAPD process must clearly identify the Medicare and Medicaid Promoting Interoperability Program objective (formerly known as the Meaningful Use)
- If PULSE will be part of the state health information exchange, this should be clearly identified and described
- Some examples of projects that are typically approved for the use of HITECH funds include:
    - Building infrastructure
    - Building specialized registries
    - Projects that encourage the use of the health information exchange
    - Projects that support emergency medical services and response in a disaster event
    - Projects that encourage interoperability among providers and/or payers

[8] https://www.medicaid.gov/sites/default/files/federal-policy-guidance/downloads/SMD16003.pdf

- Though HITECH funding must be requested through the IAPD process by the Medicaid Agency in your state, it may be implemented by another state agency such as the Public Health Department or Emergency Management Agency
- There are stringent reporting requirements for managing and reporting the use of HITECH funding
- Consider the following criteria (at a minimum) when writing an IAPD:
    - Activities must support Medicare and Medicaid Promoting Interoperability Program measures
    - Activities must support onboarding and interoperability between providers
    - Activities must focus on design, development and implementation (not maintenance)
    - Acknowledge any reuse of previous technical investments to promote sharing, leverage, and reuse of Medicaid technologies and systems

Additional Resources:

- SMDL #18-007 21st Century Cures Act Section 5006 Compliance – Provider Directories
- SMDL #18-006 Leveraging Medicaid Technology to Address the Opioid Crisis
- SMDL #18-005 Mechanized Claims Processing and Information Retrieval Systems – Reuse
- SMDL #16-010 Mechanized Claims Processing and Information Retrieval Systems – Modularity
- SMDL #16-009 Mechanized Claims Processing and Information Retrieval Systems –APD Requirements
- SMDL #16-004 Mechanized Claims Processing and Information Retrieval Systems-Enhanced Funding
- SMDL #16-003 Availability of HITECH Administrative Matching Funds to Help Professionals and Hospitals Eligible for Medicaid EHR Incentive Payments Connect to Other Medicaid Providers
- CMS Answers to Frequently Asked Questions (FAQs) Eligibility for 90 percent Federal matching funds for health information exchange activities through the Medicaid Electronic Health Record Incentive Program
- SMDL #11-004 Use of administrative funds to support health information exchange as part of the Medicaid EHR Incentive Program

Medicaid Enterprise System - MES funding, formerly Medicaid Management Information System (MMIS) funding, is available to enhance the Medicaid Enterprise system that each state Medicaid office is required to have. The MES is typically more than just a collection of modular software/applications and technology hardware. It often includes business processes that might enhance the very complex process of administering Medicaid (as a payer) in states. Unlike HITECH funding, on-going maintenance and operations funding is available at a 75 percent match rate. In addition to the IAPD, an Operations Advance Planning Document (OAPD) is also required.

Federal law provides the following options in terms of MES funding:

- 90-10 FFP funding is available for design, development, and implementation (DDI) funding for modular systems, such as disaster response platforms for patient triage and care in a declared disaster. This include web-based portals, network interfaces, and analytics capabilities.
- 75-25 FFP funding is available for the maintenance and operations of a MES system or program. This includes the following:
    - Case management
    - Care management registries
    - Manage treatment plans and outcomes
- In order to utilize 90-10 funding properly for DDI, the state agency must account for several key factors such as cost allocation, modular certification and outcome measures. If these are not met, then CMS may approve at a 50 percent (50-50) match

Below are some items to consider when pursuing MES funding:

- If considering PULSE program implementation through MES funding, it is possible to use the current HIE cost allocation approach for your state because PULSE will connect to existing networks.
- Consider using HIE outcome measures. PULSE will support these measures during a declared emergency. CMS requires 6 months of information on these measures. Ensure that you have your simple and easily measured outcomes ready and able to be recorded when you first implement PULSE.
- Be clear in your request for funding whether PULSE will only be activated during a declared emergency or used for other purposes as well.

Substance Use Disorder Prevention that Promotes Opioid Recovery and Treatment (SUPPORT) Act - In addition to HITECH Administrative and MES funding, the SUPPORT Act provides 100 percent funding for programs and tools that address the nation's opioid overdose epidemic through the design and implementation of Prescription Drug Monitoring Programs (PDMPs). To access this funding, states will add to existing Advanced Planning Document (APD) requests to the Centers for Medicare and Medicaid Services.

This funding may be available to support PULSE implementation if the state can include information from its qualified PDMP through an interoperability interface. States must also consider how PDMP access policies and related laws and regulations may affect PULSE program implementation and/or the construction of the PULSE Community technology.

Below are some items to consider when pursuing SUPPORT Act funding:

- Funding can be used for planning, implementation, interface upgrades, performance reporting and outcomes reporting
- A SUPPORT Act Advance Planning Document is required

- Funding is available through September of 2020

Additional Resources:

- FAQ SUPPORT for Patients and Communities Act, Section 5042 – Medicaid PARTNERSHIP Act https://www.medicaid.gov/sites/default/files/Federal-Policy-Guidance/Downloads/faq051519.pdf

Federal Financial Participation for Emergency Preparedness and Response

Public Health Emergency Preparedness (PHEP) and Hospital Preparedness Program (HPP) - The Hospital Preparedness Program (HPP) and Public Health Emergency Preparedness Program (PHEP) are administered out of the Office of the Assistant Secretary for Preparedness and Response (ASPR) and the Centers for Disease Control and Prevention (CDC), respectively. The HPP and PHEP programs each fund 62 cooperative agreement recipients: all 50 states, four localities, and eight territories and freely associated states. Both programs require recipients to develop and implement capability-based work plans and use their funding to build and sustain their readiness and response capacity. These programs include capabilities related to information sharing, surge management, and mass care, all of which PULSE aims to support. Both cooperative agreement programs also allow funding to be used for technology that supports these capabilities and the provision of public health and medical care to populations affected by disaster.

Additional Resources:

- https://www.grants.gov/web/grants/view-opportunity.html?oppId=313435
- https://www.cdc.gov/cpr/readiness/00_docs/PHEPNOFOFastFactsDocumentFINAL_3419.pdf.pdf

Homeland Security Grant Program (HSGP) – HSGP funding is administered by the Department of Homeland Security/Federal Emergency Management Agency (DHS/FEMA) and is intended to "enhance the ability of state, territory, local, and tribal governments to prevent, protect against, respond to, and recover from terrorist attacks and other disasters." HSGP supports the goal of Readying the Nation for Catastrophic Disasters. The HSGP is a combination of three grant programs: State Homeland Security Program (SHSP), Urban Area Security Initiative (UASI), and Operation Stonegarden (OPSG) and each has its own requirements. However, DHS/FEMA has recently shifted to organizing its national priority areas according to "Lifelines," one of which is Health and Medical. The State Homeland Security Program (SHSP) allows up to 10 investments, one of which is emergency communications that is interoperable with other systems, but more generally any investment supports closing capability gaps or sustaining capabilities identified in the THIRA/SPR process will be considered. If applying for an investment related to emergency communications, it must be tied to the Statewide Communications Interoperability Plan.

Additional Resources:

- https://www.fema.gov/homeland-security-grant-program

Contracting Options

If pursuing a third-party vendor to build, implement, deploy, or maintain any part of the PULSE program, there are several options that may be used to contract PULSE program deliverables. Below are some items to consider when selecting a contract mechanism:

- What funding source will support implementation and maintenance costs for the PULSE program?
- Will separate contracts be required for implementation and maintenance requirements?
- Which agency (i.e., who) will handle contracting and procurement processes?
- Are joint agency sponsors required?

Types of Contracts

Request for Procurement (RFP) - An RFP is a document that defines the goods and services that need to be received by the state, etc. The procurement request package typically includes a detailed statement of work, business requirements and specifications. This forms the basis for an invitation to submit a bid for the work. Sometimes RFPs are written in a broad manner so that those responding to the RFP may present their ideas and strategies for delivering within confines around those strategies.

State governments typically have different laws around how RFPs are issued. If it is determined that a request for procurement is required for PULSE, this will typically add in time in terms of allowing vendors the appropriate amount of time to reply, reviewing the proposals, responding to bidders' questions, bidder conferences, etc.

Questions to Consider:

- Does the state have a designated health technology funding policy and structure (e.g., designated entity)?
- If the state must utilize the RFP process, are there adequate staffing resources to support this process?
- Does the time required to complete an RFP process align with your implementation goals?
- Does the funding that has been allotted for this procurement allow a sole source procurement or must the it be competitive?
- Does the state allow requests for information instead of RFPs?

Request for Information (RFI) – The RFI is primarily used to gather information to help decide on what steps to take next in terms of a procurement. RFIs are seldom the final stage of the procurement and are often instead used in combination with the RFP process. For instance, if the state is not certain that a service or product is a sole source, the entity may opt to issue an RFP with a quick turnaround time to gauge the market in terms of product or service availability. If only one response is received, the state could determine that this procurement is indeed a sole source and convert the RFI to a contract document with the responsive vendor. This may result in a quicker turnaround time and less strain on state resources. States should confirm before proceeding down this path whether converting an RFI to a contract is allowed in the respective state.

Sole Source – A sole source procurement can be defined as any contract entered without a competitive process, based on a justification that only one known source exists or that one single supplier can fulfill the requirements. Sole source procurements can be complicated depending on the requirements for a state government. Typically, most sole source procurements require specific documentation on why this service or product is deemed the sole option. Sole source procurements may also require extensive review and approval from a variety of levels of state government, up to and including the state attorney general's office. State agencies may also have additional requirements and documentation pertaining to sole source procurements on top of or outside of the state government requirements. Documented due diligence in terms of extensive research on the availability of a product or service is also typically necessary.

Questions to Consider:

- Does the state allow sole source procurements?
- If so, are sole source procurements available with for profit vendors or only with sole source vendors?
- What is the specific documentation needed in order to allow a sole source procurement?
- Who needs to approve or review the sole source procurement?

Document Revision History

Version	Date	Description
1.0	27 January 2020	Initial release
2.0	May 21, 2020	Interim release 1