P3N
Technical Requirements
PA eHealth Partnership Program

Subject: P3N Technical Requirements	**Version:** v.4d
Status: Effective January 1, 2024	**Creator:** Allen Price
Approval Date: October 4, 2023	**Contact:** Kay Shaffer (kashaffer@pa.gov)
Original Issue Date: April 13, 2015	**Last Review Date:** October 4, 2023
Related Documents:	-Terms and Definitions -Pennsylvania eHealth Partnership Program Uniform Participant Agreement v.4d

1 Introduction

This document describes the technical requirements required for certification specific to the Pennsylvania Department of Human Services' eHealth Partnership Program (PA eHealth) and the Commonwealth of Pennsylvania. As potential Certified Participants (CPs) begin the process to connect to the Pennsylvania Patient & Provider Network (P3N), decisions such as participant connection type and Services used are documented when onboarding to the P3N. This document provides additional technical information. Query and Retrieve interfaces to the P3N rely on the Integrating the Healthcare Enterprise (IHE) IT Infrastructure (ITI) Technical Framework (https://www.ihe.net/resources/technical_frameworks/#IT). The P3N Public Health Gateway (PHG) and the Admission Discharge Transfer (ADT) services rely on Health Level 7 (HL7) version 2.X messages. Any references to ITI Specifications in this Agreement also encompass subsequent versions. This document summarizes technical requirements in support of the testing documentation provided during onboarding to PA eHealth services.

2 P3N Master Patient Index (MPI)

2.1 Register Patient

2.1.1 CPs shall register and update the P3N Patient Demographic Feed using one of the following Participant feed types:

- Patient Identifier Cross Referencing (PIX)
- Admission, Discharge, & Transfer (ADT)

2.1.2 If CP elects to use PIX, CPs shall register and update patients (Data Provider) using PIX IHE specifications. Patient feeds to the P3N shall include PIX v3 (ITI-44) or PIX v2 (ITI-8).

2.1.3 If CP elects to use the P3N Admission, Discharge, Transfer (ADT) Encounter Service, patient demographics shall be provided using HL7 2.X specifications.

2.1.4 As patients are registered, updated, or deleted at the CP MPI, the CP shall perform registrations and updates at the P3N MPI.

2.1.5 CP shall merge patients in the P3N as they are merged in the CP HIE.

2.1.6 If there is a requirement to split or unmerge a patient, the CP will address this locally at their HIO and at the P3N using P3N support processes.

2.1.7 If patients are removed from the CP MPI, the CP shall initiate the removal of the CP patient from the P3N MPI using P3N support processes.

2.1.8 Patient Data fed to the P3N MPI shall include the following:

1) HIO Patient ID (R)
2) First Name (R)
3) Middle Name/Initial (R2)
4) Last Name (R)
5) Date of Birth (DOB) (R)
6) SSN (if available, or last 4 digits) (R2)
7) Medicaid Recipient Number (R2)
8) Gender (R2)
9) Address (Address Line 1, Address Line 2, State, Zip Code) (R)
10) Phone (R2)
11) Race (R2)

(R – Required, R2 – Required if data present)

2.1.9 PA eHealth and CP will determine by mutual agreement if CP patient Data is preloaded and available at go-live. If the P3N MPI is populated via bulk upload, the file will contain the date and time of last update to assure that data is the most recent available.

2.1.10 CP shall register all Patient IDs and demographic data created after the CP go-live date in the P3N.

2.2 Query For Patient

2.2.1 CP shall query the P3N for patients using IHE specifications.

2.2.2 CP shall choose PIX v3 (ITI-45), PIX v2 (ITI-9) or XCPD (ITI-55) to query for a patient at the P3N.

2.2.3 A CP that elects to use PIX to query for P3N patient IDs must use the CP Patient IDs.

2.2.4 A CP that elects to use XCPD to query for P3N patients must use the same patient demographics used during PIX registration or updates to the P3N.

2.2.5 A CP that elects to use XCPD to query for P3N patients may use the same XCPD gateway and digital certificates used by the Sequoia Project's eHealth Exchange.

2.3 PA eHealth will provide P3N secure connection endpoints using Transport Layer Security (TLS 1.2 or higher) mutual authentication to the CP to register, update, and query for patient data within the P3N MPI.

2.4 CP shall maintain Audit Trail and Node Authentication (ATNA) log records as specified in the IHE standards for all PIX or XCPD transactions with the P3N for the intention of auditing and reporting.

3 P3N Query and Retrieve Connectivity Types

3.1 CP shall connect to the P3N and share all available Data with other CPs as determined by one of two Participant connection types:

- Cross-Enterprise Document Sharing (XDS)
- Cross-Community Access (XCA)

3.2 P3N Cross-enterprise Document Sharing (XDS) Participants

3.2.1 CP shall register, query, and retrieve patient's clinical documents from the P3N using IHE XDS specifications.

3.2.2 CP shall register stable (ITI-42) or on-demand (ITI-61) clinical documents in the P3N XDS Registry.

3.2.3 As documents are registered, updated or deleted at the CP registry, the CP shall update the P3N XDS Registry.

3.2.4 CP shall provide metadata in accordance with attributes defined in the IHE XDS specifications as documents are registered in the P3N XDS Registry.

3.2.5 CP shall provide metadata values in accordance with the whitelist of values required by PA eHealth. The whitelist of values will be provided by PA eHealth's technology vendor during interoperability testing, based on the codes.xml file maintained by the federal Connectathon project.

3.2.6 CP will use the confidentially code metadata attribute to tag registry entries in the P3N XDS Registry as anything but Normal ("N") when registering clinical documents with the presence of Super Protected Data (SPD). (e.g., HIV and AIDS status, mental health, or substance abuse related care). If CP cannot appropriately tag clinical documents containing SPD, then those documents will not be registered or available from the P3N. The current confidentiality codes reference can be found at: https://www.hl7.org/fhir/v3/Confidentiality/cs.html

3.2.7 PA eHealth and CP will determine by mutual agreement what legacy documents will be registered in the P3N to be preloaded and available to other CPs at go-live.

3.2.8 CP shall use the P3N Patient ID to query (ITI-18) the P3N for clinical documents associated with that patient.

3.2.9 CP shall retrieve documents (ITI-43) from the P3N based on the query response.

3.3 P3N Cross Community Access (XCA) Participants

3.3.1 CP shall query and retrieve patient's clinical documents from the P3N using IHE XCA specifications.

3.3.2 CP shall use the P3N Patient ID to query (ITI-38) the P3N for clinical documents associated with that patient.

3.3.3 CP shall retrieve documents (ITI-39) from the P3N based on the query response.

3.3.4 CPs that elect to use XCA to query and retrieve documents from the P3N may use the same XCA gateways and digital certificates they use in the Sequoia Project's eHealth Exchange.

3.3.5 CPs shall not use the XCA connections established through the P3N onboarding process to exchange clinical Data with one another independent of the P3N Certification program.

3.4 PA eHealth will provide P3N secure connection endpoints using TLS mutual authentication to the CP to query for and retrieve documents from other CPs.

3.5 CP shall make available for document retrievals all available data from their clinical document repository through a secure endpoint.

3.6 CP shall maintain Audit Trail and Node Authentication (ATNA) log records as specified in the IHE standards for all XDS and XCA transactions with the P3N for the intention of auditing and reporting.

4 P3N Query Document Types

4.1 All clinical documents created on and after the CP go-live date with the P3N shall be available to other P3N CPs.

4.2 CP clinical documents shall be available to a P3N query whenever the CP system is available to its internal users, except during regularly scheduled maintenance windows or downtime. If the CP will be unavailable for P3N queries beyond normal maintenance periods, the CP shall notify PA eHealth and all other CPs.

4.3 As the CP is queried for documents by its Member Organizations (MOs), the CP shall in turn query the P3N for documents for that patient.

4.4 The Pennsylvania eHealth Partnership Program maintains a community owned Super Protected Data (SPD) codes list that can be used to filter drug and alcohol, HIV/AIDs, and behavioral health information.

4.5 Purpose of Use

4.5.1 CPs shall use metadata values based on HL7 standards to support the requirements for appropriate document sharing as defined in the Pennsylvania eHealth Partnership Program Uniform Participant Agreement (PAR). While the capability to share data for multiple purposes is available, the obligations under HIPAA fall on the CP and its MOs.

5 P3N Query Document Sharing

5.1 Reciprocal Duty to Respond

5.1.1 All CPs that request, or allow their Authorized Users to request, PHI through the P3N shall have a corresponding reciprocal duty to respond to queries for PHI and/or clinical documents from other CPs and their Authorized Users, including all available data.

5.2 The CP may respond to a query by either providing the requested Data or by responding that the Data is not available or cannot be exchanged.

6 Digital Certificates

6.1 P3N secure connection endpoints are protected by network whitelisting endpoints and requires Transport Layer Security (TLS 1.2 or higher) mutual authentication.

6.2 TLS mutual authentication requires the exchange and import of digital certificates from participating parties, PA eHealth and the CP.

6.3 Certificate Policies

6.3.1 CP may delegate the digital certificate management tasks to a Third Party or Parties Certificate Authorities nationally recognized (no self-signed certificates).

6.3.2 CP shall use digital certificates from trusted sources for identity services.

6.3.3 CP shall securely manage associated X.509 digital certificate private keys.

6.3.4 CP certificates shall be published, housed and validated by a Certificate Authority (CA).

6.3.5 CP may perform CA services for the use of its own organization and its MOs. If CP is acting as its own CA, it must have policies in place for managing certificates.

6.3.6 For connection to the P3N, digital certificates shall be chained to root certificates issued from the approved vendors listed by the Federal Public Key Infrastructure (FPKI) or Trust Framework Services (TFS) (Trust Services (idmanagement.gov)).

6.3.7 CP digital certificate(s) shall be used to encrypt PHI when the Data is at rest or in transit. Wildcard or multi-domain certificates may not be used to exchange PHI through the P3N.

6.3.8 CP shall have and adhere to policies and procedures that protect against any anticipated threats or hazards to the security or integrity of digital certificates in compliance with their certificate policy guidelines.

6.3.9 CP shall provide digital certificate policies to PA eHealth upon request.

6.3.10 CP shall provide the updated certificates to PA eHealth for the purposes of maintaining connectivity to the P3N.

6.4 Certificate Revocation

6.4.1 CP shall disable any digital certificates it provides to connect and access any services of the P3N, or connection to other CPs of the trust community, in the event of any security issue, policy violation, certificate expiration, or termination of business relations.

6.4.2 CP shall ensure that any registry entries of revoked digital certificates are updated or corrected.

6.4.3 CP may utilize Online Certificate Status Protocol (OCSP) transactions in conjunction with or in lieu of publishing a Certificate Revocation List (CRL).

6.4.4 Entities requesting the trust status of disabled certificates shall be notified by PA eHealth of the certificates' status.

6.4.5 If the CP uses a CRL to maintain disabled certificates, the CP shall make the status of disabled/untrustworthy certificates discoverable by P3N entities.

6.4.6 CRLs shall be published and maintained by Certificate Authorities on a periodic basis of no less than once every 24 hours.

6.4.7 CRLs shall have a defined lifespan of no more than 24 hours for which they are valid.

6.4.8 CRLs shall list information sufficient to identify all disabled certificates which are no longer trustworthy. Digital certificates listed on a CRL shall have status indicators of either "Revoked" (irreversibly disabled) or "Hold" (reversibly disabled).

7 P3N Provider Directory (PD)

7.1 P3N hosts a Provider Directory (PD) that is accessible from the P3N system portal.

7.2 CP may provide access to the P3N PD to users, which may include clinicians, support staff, and administrative staff.

7.3 The P3N PD hosts provider information on both individual providers as well as organizations.

7.4 CP may submit both individual and organizational Health Care Provider Data to PA eHealth to be included in the P3N PD.

7.5 Individual PD entries are defined as individual Health Care Providers who are licensed or otherwise authorized by a state within the United States to provide health care services or support public health initiatives.

7.6 Organizational PD entries are defined as:

1) Health Care Provider organizations (e.g., hospitals, clinics, etc.)
2) Other health care organizations (e.g., health plans, public health, etc.)
3) HIOs (e.g., regional HIE operators, etc.)
4) Other organizations involved in HIE (e.g., Business Associates, clearinghouses, HISPs, etc.)

7.7 When submitting Health Care Provider records to PA eHealth, the file format shall be a comma-delimited file.

7.8 Health Care Provider Attribute Data is defined in the IHE Healthcare Provider Directory (HPD) Specification.

Organizational Provider attributes are as follows:

1) Organization Identifier (R)
2) Organization Name (R)
3) Organization Type (O)
4) Organization Type Description (O)
5) Organization Status (Active, Inactive) (O)
6) Organization Contact (O)
7) Organization DIRECT or medical records delivery email address (O)
8) Organization Practice Address (R2)
9) Organization Billing Address (O)
10) Organization Mailing Address (R2)

11) Provider Language Supported (O)
12) Organization Specialty (O)
13) National Provider Identifier (NPI) Number (R2)
14) PA License Number (R2)
15) Organization Business Phone (R2)
16) Organization Fax (R2)

(R – Required, R2 – Required if data present, O – Optional)

Individual Provider attributes are as follows:

1) Unique Individual Identifier (R)
2) Provider Type (R)
3) Provider Type Description (R)
4) Provider Status (Active, Inactive, Retired, Deceased) (O)
5) Primary Provider Name (R)
6) Provider Title (O)
7) Provider First Name (R2)
8) Provider Middle Name (O)
9) Provider Last Name (R)
10) Provider Language Supported (O)
11) Provider Gender (O)
12) Provider DIRECT or medical records delivery email address (O)
13) Provider email address (O)
14) Provider Facility Name (R2)
15) Provider Mailing Address (R2)
16) Provider Billing Address (O)
17) Provider Practice Address (R2)
18) Provider Practice Organization (O)
19) Provider Business Phone (R2)
20) Provider Fax (R2)
21) Provider Specialty (O)
22) National Provider Identifier (NPI) Number (R2PA License Number (R2)

(R – Required, R2 – Required if data present, O – Optional)

7.9 If a CP participates in the Provider Directory, the CP shall submit Health Care Provider Data files to PA eHealth at least twice per year via secure File Transfer Protocol (sFTP) to be imported into the P3N PD.

7.10 PA eHealth will report errors encountered when uploading Data and work with the CP to resolve the entry.

7.11 CP Providers not located within the borders of the Commonwealth of Pennsylvania may participate, subject to applicable state and federal laws.

7.12 CP, or its MOs, shall enroll its member individuals and organizations in a secure manner that includes verification of the information used to populate the PD.

7.13 CP shall manage its internal PD to maintain current listings.

7.14 CP may delegate maintenance responsibility to the providers (or their delegated authorities).

7.15 CP shall implement security policies and procedures on its internal provider directory that provide for the following:

1) Authorized individuals have access to the Data for purposes of updates and changes.
2) Data contained in the PD is appropriately protected from unauthorized changes, and changes are logged.

8 Public Health Gateway (PHG) Service

8.1 The P3N provides a single point of entry to CPs and their MOs for the purpose of sending public health information to the Commonwealth health reporting registries.

8.2 CP must be certified before using the PHG service in a production environment.

8.3 CP may use the P3N to submit to and query the following public health reporting registries (additional specialized registries may be added over time):

1) PA DOH Immunization Registry
   - Submission and Query
2) PA-NEDSS for Electronic Laboratory Reporting
   - Submission Only
3) PA DOH Cancer Registry
   - Submission Only
4) PA DOH Prescription Drug Monitoring Program (PDMP)
   - Query only

8.4 MOs that submit to public health registries through CPs must qualify message content with commonwealth registry owners prior to using the PHG services in production.

8.5 The P3N will not interrogate the data in the message body nor decrypt it. The P3N will pass the message on to the public health reporting registry using the routing information contained in the message header.

8.6 PHG messages are synchronous. Should delivery not be possible, the sender will receive an error and will need to resubmit. The P3N does not store the message for a future attempt to send it.

8.7 The P3N will send a response to the sender once the message is delivered to the appropriate registry.

9 P3N Admission, Discharge, Transfer (ADT) Encounter Service

9.1 CP must be certified before using the ADT service in a production environment. Interstate P3N Participants must enter into a data sharing agreement with the Pennsylvania Department of Human Services (DHS) and undergo a rigorous ADT service onboarding.

9.2 The ADT service matches patients identified at the P3N MPI from the source CP to patients registered at destination CPs. For Interstate Participants, the ADT service forwards messages based on the patient's state of residence.

9.3 The ADT service will send ADTs in near real-time from one participant to other participants and will hold ADTs not routed for two weeks.

9.4 The ADT service will provide a secure P3N connection endpoint to the participants for submitting ADTs.

9.5 Each participant shall provide a secure destination endpoint to receive ADTs forwarded from the P3N through a secure VPN (HL7 TCP) interface.

9.6 Only HL7-based ADT version 2.X transactions for patients sent to P3N will be sent to participants from the P3N ADT service.

9.7 PA eHealth's vendor will provide onboarding documentation upon project startup to onboard to the ADT service. This documentation will include required and optional fields, and value sets for use in the ADT messages.

9.8 If a CP elects to use this service, it shall contribute ADT messages to other CPs for consumption and must comply with the requirements and restrictions related to sharing restricted self-pay data with health plans.

9.9 CP shall use the ADT service to enable real-time electronic notification services at its CP.

9.10 PA eHealth will provide monthly message traffic activity reports to participating CPs.

9.11 CP shall log all transactions to the P3N ADT service.

9.12 The Pennsylvania eHealth Partnership Program maintains a community owned Super Protected Data (SPD) codes list that can be used to filter drug and alcohol, HIV/AIDs, and behavioral health information from ADT messages.

10 Security Audits and Risk Assessment

10.1 CP shall undertake annual security audits and risk assessments using an independent, qualified, organization to ensure appropriate technical, physical and administrative safeguards.

10.2 PA eHealth in consultation with HIETCC will verify the third-party entities have sufficient expertise and qualifications to perform security audits and risk assessments.

10.3 When CP certifies to connect to the P3N, it shall provide PA eHealth with the results of its most recent security audit and risk assessment. The results must be dated within 12 months from the date of submission of the Application to PA eHealth.

10.4 CP shall make available upon request to PA eHealth the results of annual security audits and risk assessments.

11 Service Level Agreements (SLAs)

11.1 CP shall establish and maintain Service Level Agreements (SLAs) with all MOs that use their services. CP shall use best efforts to meet industry standards for SLA metrics. SLAs should include, at a minimum, the following:

11.1.1 Service availability – Calculated and reported as a percentage that represents the service uptime

11.1.2 Service restoration – Time spent in repairing a fault or restoring the service

11.1.3 Continuous monitoring – Constant monitoring and verification that service levels are met

11.1.4 Help desk coverage – Issues are communicated and logged, tracked, and resolved within specific timeframes

11.1.5 Response times – Services respond in an agreed upon timeframe

11.2 PA eHealth may ask CPs to provide their current SLAs and/or current SLA reports.

11.3 CP shall provide maintenance notifications to PA eHealth and P3N Participants when their systems are scheduled to be unavailable.

12 Advance Care Planning Documents Registry

12.1 The P3N will host in its clinical data repository a statewide Advance Directives Registry and repository that will allow CPs, PA eHealth, and Health Care Providers to register Advance Directives, Pennsylvania Orders for Life Sustaining Treatment (POLST), and Do-Not-Resuscitate (DNR) Orders in the P3N which will be discoverable and retrievable by querying the P3N.

12.2 Advance Directive Documents will be represented by HITSP C62 or the C-CDA unstructured document template.

12.3 Advance Directive Documents will be registered at the P3N through one of two ways:

12.3.1 Scanned, signed document is provided to PA eHealth by Patient, Provider, or CP to manually upload document into the P3N CDR.

12.3.2 HIO performs a Provide and Register Document Set (ITI-41) at the P3N Cross-Enterprise Document Sharing (XDS) endpoint.

13 Care Plan Registry

13.1 The P3N will host in its clinical data repository a statewide Care Plan Registry and repository that will allow Medicaid Managed Care Organizations (MCOs), Health Care Providers, and PA eHealth to register patient Care Plan documents that are discoverable and retrievable by querying the P3N. DHS requires physical health and behavioral health MCOs to develop and share care plans for complex patients.

13.2 Care Plan Documents will be represented by the C-CDA care plan document template, HITSP C62 or the C-CDA unstructured document template.

13.3 Care Plan Documents will be registered at the P3N through one of two ways:

13.3.1 Care Plan document is provided to PA eHealth by Provider or CP to manually upload document into the P3N CDR.

13.3.2 HIO performs a Provide and Register Document Set (ITI-41) at the P3N Cross-Enterprise Document Sharing (XDS) endpoint.