Note: While the Coordinating Committee approved this specification on 10/1/2016 (not limited to trial use) this specification needs to be revisited with additional community input once a real-world implementation is underway.

eHealth Exchange Personal Health Record (PHR) Profile

Version: 8

Date Updated: 2016-01-19

Status: DRAFT for Sequoia Staff Review

Authors: Eric Heflin (lead author), Jen Rosas, Gonzalo Hernando

Contents

Executive Summary

Since its very inception, the eHealth Exchange has envisioned PHRs being part of the network. This Personal Health Record (PHR) Profile is built around the primary use case of enabling End-Users with the ability to interact with a large national network of states, federal agencies, and more using the eHealth Exchange. The anticipated use cases are defined in this document, along with detailed sub-use cases, the technical specification, security model, Patient privacy considerations, special security considerations related to this use case, and more. This document is intended to be built upon lower-level eHealth Specifications including Messaging Platform, Authorization Framework, and Access Consent Policies.

This profile enables PHRs, and more specifically PHR vendors on behalf of their End-Users, with the ability to share information with other eHealth Exchange Participants electronically, while also enabling the PHR End-User to obtain information from other eHealth Exchange Participants. PHRs can either act as either a data source, or a data consumer, or both. To avoid performance problems, PHRs are required to respond to requests within 10 seconds. PHRs are required to send a PurposeOfUse and a Role code indicating that the request is pursuant to Patient authorization. The Patient authorization is made available to disclosing parties by the PHR system using the eHealth Exchange Access Consent Policies (ACP) profile.

A number of policy issues have been identified and are called out for future refinement. These policy issues also are defined in the PHR profile, in an implementable way, to allow precise deployment of this profile in the absence of policy to the contrary.

In addition, a number of important topics have identified and put in an appendix for future consideration.

Audience

This document's primary target audience are those that are implementing, testing, or operating an eHealth Exchange technical end point providing for one-way or bi-directional exchange, where at least one of the parties to the exchange is a Personal Health Record system. It assumes at least a high-level understanding of the eHealth Exchange's business and clinical use cases, architecture, functional capabilities, security model, and legal / trust framework. In order to implement this specification, one will need the information contained herein, plus additional information contained in the underlying documents referenced in the Specifications section. Addition information about the eHealth Exchange, including recorded webinars, presentations, and other educational material, may be found on the eHealth Exchange web site, at http://www.ehealthexchange.com. For additional information, you may also reach the eHealth Exchange support staff by sending an email to administrator@ehealthexchange.com.

Document Conventions

In this document, to avoid ambiguity between normative and non-normative statements, there will specific conformance statements called out in this document, following the format CONF####.

```
Source code examples are presented using a mono-spaced font, in a gray
background such as this.
```

[Note to reviewers: Please look for text like this and provide specific feedback.]

Definitions

The following potentially unfamiliar terms are used herein.

Access Consent Policies (ACP) – An eHealth Exchange specification defining a workflow and associated structural message and structural content components allowing a person's consent or authorization information to be conveyed from one Participant to another. See the Specifications section.

End-User – The PHR logged-in person which may either be the Patient, or may be acting on behalf of the Patient (such as a parent acting on behalf of a minor child).

Patient – The actual subject of the clinical data exchange.

Patient Discovery (PD) – The eHealth Exchange Patient Discovery specification. See the Specifications section.

Personal Health Record (PHR) – A software system providing a view of clinical data to end user consisting of patients, or a patient's authorized representatives, with optional additional capabilities.

Query for Documents (QD) – The eHealth Exchange Query for Documents specification. See the Specifications section.

Retrieve Documents (RD) – The eHealth Exchange Retrieve Document specification. See the Specifications section.

[Reviewers: What additional terms should be defined?]

Methodology

This specification was created using an open, transparent, vendor- and technology-neutral process. All meetings held during the development of this profile were public. Several calls for participation were announced in eHealth Exchange work groups meetings, and via the associated email lists. All interested organizations and individuals were invited to participate. A formal Software Design methodology was employed, first gathering business and clinical requirements from identified stake holders. These requirements were then documented as use cases, and then used to generate requirements, and then a system design and this specification designed to meet those requirements. A validation plan to allow for independent verification and validation of these capabilities was specified. Public feedback was solicited from the broad community of eHealth Exchange Participants, the vendors supporting them, and the public. The final version of the PHR Profile will be created via a public dispositioning process and made freely available for use by anyone. All throughout this process critical comments were actively requested and incorporated into this document.

Use Cases

[Reviewers: We plan to provide moderately detailed formal use cases in this section. Do you agree with this approach?]

1. A PHR deployment, on behalf of a patient, and with a patient's authorization, seeks information from one or more eHealth Exchange Participants in response to a *query* from the PHR to the selected data sources known to the PHR.
    - Alternate flows:
        - Automatically initiated by the PHR
        - One time vs. re-occurring queries
2. The PHR acts as a data source, and responds to other eHealth Exchange Participants for non-Patient-entered data stored in the PHR.
    - Alternate flows:
        - The PHR responds with Patient-entered or curated data (not allowed by this version of the PHR profile due to lack of standard approaches to indicate Patient mediated data)

[Reviewers: Should we consider other use cases, such as "push", or PHR enrollment?]

Patient Privacy Considerations

The PHR shall permit query for documents only on behalf of registered End-Users and solely for the benefit of the End-User as per the DURSA Permitted Purposes clause. The eHealth Exchange DURSA, permitted purposes include "Uses and disclosures pursuant to an Authorization provided by the individual who is the subject of the Message or such individual's personal representative as described in 45 C.F.R. § 164.502(g) of the HIPAA Regulations."

CONF#### The PHR shall not use the eHealth Exchange to perform a query for any data other than as allowed by the DURSA Permitted Purposes clause.

CONF#### The PHR shall obtain a HIPAA compliant authorization from the End-User.

CONF#### The Patient's or End-Users authorization form will be made available to the Responding Gateway via the Access Consent Policies profile.

The Responding Gateway, which is acting as the disclosing party, has the opportunity to retrieve, inspect, and act on this authorization form. However, the Responding Gateway is not required to retrieve the Patient authorization form by the PHR Profile.

CONF#### An PHR acting as an Initiating Gateway shall import personal health information from Responding Gateways into an End-User's record.

UDDI/Directory Considerations

The current eHealth Exchange Web Services specification applies to the PHR Profile.

CONF#### PHR Implementers SHOULD use the current UDDI directory to identify Participant technical end points.

CONF#### PHR Implementers MUST use the current UDDI directory to list their own technical end points.

Care Summary Content

The existing eHealth Exchange content policy applies which is that content should be exchanged using a standards-based format, if such a format is available.

[Reviewers: Are they any additional constraints that should be placed on PHR generated content? Should we allow, or disallow, the PHR from responding with content that was potentially created or modified by the End-User or the Patient? Should we require the use of HITSP C-32 and/or IHE/HL7 C-CDA?]

Standards and Specifications

The PHR Profile is based upon the existing eHealth Exchange specifications.

All eHealth Exchange specification may be found at http://ehealthexchange.com/resources/exchange-specifications or its successor page.

eHealth Exchange 2011 series of profiles:

1. Web Services Registry Web Service Interface Specification v 3.1 3/6/2012 [PDF – 405 KB]
2. Messaging Platform v3.0 approved by NTCon 6/27/2011 [PDF – 232 KB]
3. Patient Discovery v2.0 approved by NTCon 6/27/2011 [PDF – 234 KB]
4. Query for Documents v3.0 approved by NTCon 6/27/2011 [PDF – 201 KB]
5. Retrieve Documents v3.0 approved by NTCon 6/27/2011 [PDF – 153 KB]
6. Authorization Framework v3.0 approved by NTCon 7/25/2011 [PDF – 226 KB]
7. Web Services Registry v3.0 approved by NTCon 7/25/2011 [PDF – 376 KB]

eHealth Exchange 2010 series of profiles:

1. Access Consent Policies Production Specification – v1.0 [PDF – 154 KB]

Other specifications are incorporated by the eHealth Exchange specifications, such as standards by IHE International, HL7, OASIS, W3C, and others. Key standards include IHE ATNA, XUA, XCPD, XCA, BPPC, IHE/HL7/ONC C-CDA, and HITSP C32.

CONF#### PHR vendors MUST the 2011 eHealth Exchange specifications.

CONF#### PHR vendors MAY support the 2010 eHealth Exchange specifications.

[Reviewers: Please provide comments on this topic. Should the PHR profile only support 2011 specifications, for example? Metric: eHealth Exchange Support Staff records indicate that approximately 28 organizations only support the 2010 specification sets. At this point, 110 organizations are live and in production. Thus approximately 82 production Participants support 2011 only, or 2010 and 2011]

Technical Specification

PHR Initiating Gateways

CONF#### PHR Implementers acting as Initiating Gateways, MUST support the eHealth Exchange 2011 Authorization Framework, Messaging Platform, Patient Discovery, Query for Documents, and Retrieve Documents specifications.

CONF### Implementers must also support the Initiating Gateway role of the Access Consent Policies specification.

Non-normative: The ACP specification was created in 2010 and remains the current version.

CONF#### PHR Implementers acting as Initiating Gateways, MAY support the eHealth Exchange 2010 Authorization Framework, Messaging Platform, Patient Discovery, Query for Documents, and Retrieve Documents specifications.

CONF#### PHR Implementers acting as Initiating Gateways, MUST transmit a SAML assertion PurposeOfUse value of “REQUEST”.

PHR Responding Gateways

CONF#### PHR Responding Gateways, MUST support the eHealth Exchange 2011 Authorization Framework, Messaging Platform, Patient Discovery, Query for Documents, and Retrieve Documents specifications.

CONF#### PHR Responding Gateways MUST support the eHealth Exchange Access Consent Policies specification.

CONF#### PHR Responding Gateways, MAY support the eHealth Exchange 2010 Authorization Framework, Messaging Platform, Patient Discovery, Query for Documents, and Retrieve Documents specifications.

CONF#### PHR Responding Gateways, MUST respond to requests for Patient data for the PurposeOfUse of “TREATEMENT”, “EMERGENCY”, “DISASTER” and they MAY respond to requests for other PurposeOfUse values such as “CLAIMS”, “OPERATIONS”, etc.

SAML Attributes

CONF#### The following SAML attributes MUST be conveyed from the PHR Profile Initiating Gateway to the Responding Gateway:

1. purposeofuse (urn:oasis:names:tc:xspa:1.0:subject:purposeofuse)
2. subject-id (urn:oasis:names:tc:xspa:1.0:subject:subject-id)
3. organization (urn:oasis:names:tc:xspa:1.0:subject:organization)
4. organization-id (urn:oasis:names:tc:xspa:1.0:subject:organization-id)
5. homeCommunityId (urn:nhin:names:saml:homeCommunityId)
6. role (urn:oasis:names:tc:xacml:2.0:subject:role)
7. accessconsentpolicy (see the eHealth Exchange Access Consent Policies specification)
8. instanceaccessconsentpolicy (see the eHealth Exchange Access Consent Policies specification)

Non-normative: These values are designed to enable high-resolution audit logging and to enable detailed policy and access control determination decisions. Non-repudiation of transaction activity is accomplished by retained audit logs, and signed SOAP message elements.

CONF#### Where End Users are distinct from Patients, the PHR Vendor MUST ensure the appropriate authorization is in place.

CONF#### The PurposeOfUse SAML attribute value shall be ‘REQUEST’ as per the eHealth Exchange Authorization Framework Specification v3.0 http://sequoiaproject.org/wp-content/uploads/2014/11/nhin-authorization-framework-production-specification-v3.0.pdf table 3.3.2.6-1 and it is defined as the individual (pursuant to authorization).

CONF#### The role code SAML shall be "116154003" with a displayname of "Patient" as per the eHealth Exchange Authorization Framework Specification v30, as per HITSP C80 Table 2-155 with a value set OID of 2.16.840.1.113883.3.18.6.1.15. In version 2.0 of the Authorization Framework Specification http://sequoiaproject.org/wp-content/uploads/2014/11/nhin-authorization-framework-production-specification-v2.0.pdf in table 4.

Patient Matching

CONF#### The End-User and the Patient MUST be identity proofed to the applicable version of the NIST 800-63 publication series, level 3 or above (e.g. an employee that has a background check and I-9 verification of employment eligibility.)

CONF#### The PHR MUST implement technical controls to minimize the likelihood of an End-User from obtaining information other than their own (e.g. In the event of a hospital records error or similar event where a Patient was incorrectly linked or incorrectly merged, a Patient may receive the wrong information).

CONF#### The PHR MUST make the Patient trait criteria used for matching immutable (i.e., should birth date be used for matching logic, the End-User shall not be able to change birth date to a different value and re-query for documents.) In addition, the PHR will deploy Patient matching logic in such a way as to minimize the possibility of ambiguous matches. (e.g. the PHR will match on traits such as an identifier).

CONF#### PHR Profile implementers MUST support the Patient Matching Minimal Acceptable Rules as per The Sequoia Project Framework for Patient Identity Management.

CONF#### PHR Initiating Gateways and Responding Gateways MUST exchange all of the following demographic traits:

1. Patient Legal First Name
2. Patient Legal Middle Name
3. Patient Legal Last Name
4. Patient Legal Date of Birth
5. Patient Legal Administrative Gender
6. Patient Legal Zip Code

CONF#### PHR Initiating Gateways and Responding Gateways MUST exchange all of the following demographic traits unless not allowed by applicable law:

1. Social Security Number in the format of a single integer number
2. Telephone Number and Telephone Number Type (home, mobile, work, etc.) in the format as specified in the *3.1.5.1 Coding Telephone Numbers* in the eHealth Exchange Patient Discovery specifications, including the telephone type (home, mobile, work, etc.) as a required if known attribute of the telephone number
3. USPS Street Address Line 1

4. USPS Street Address Line 2
5. USPS Coded City
6. USPS Coded State
7. MPI, EMPI, and other known identifiers in the format as specified in section *3.1.4 Specifying Patient Identifier in the Request* in the eHealth Exchange Patient Discovery specifications
8. State Drivers Licenses

CONF#### Default or temporary Patient name demographics traits, MUST NOT be exchanged by either Initiating Gateways or Responding Gateways.

CONF#### Patient Demographic Changes MUST NOT be performed by Patients or End-Users, they must be performed by PHR Vendor administrative staff.

CONF#### PHR Responding Gateways MUST only return exact (very high confidence) matches.

CONF#### PHR Responding Gateways MUST only return one match may be returned per assigning authority.

Security Considerations

Threat Models

Threat: A Patient that has the same legitimate demographics as a VIP or another Patient.

Mitigation: A PHR admin performs the linking manually if the Patient’s matching is not exact.

Threat: Specific to an outbound request initiated by a Patient results in an impermissible information disclosure about the data from a different Patient.

Mitigation: The End-User and Patient must be identity proofed to a high level of assurance, and the Patient is not allowed to change their Patient Discovery matching trait information.

Threat: An attacker claims a target’s identity attributes (impersonation).

Mitigation: Sufficient demographics must be captured by the PHR in order to uniquely identify the Patient uniquely.

Threat: Additional threats due to ambiguous matches.

Mitigation: Ambiguous matches are not permitted by this version of the PHR Profile.

Threat: ID Proofing may not be sufficient to prevent attacks via impersonation.

Mitigation: The PHR Profile request NIST 800-63 level 3 or 4.

Threat: Unintentional Patient traits errors in the PHR or PHR data.

Mitigation: PHR Implementer must implement internal quality assurance processes to eliminate this threat.

Threat: An attacker uses Man-In-The Middle (MITM), Denial of Service, or other similar attacks.

Mitigation: The existing eHealth Exchange security assessment applies to the PHR Profile, and includes a mitigation for these threats.

Threat: PHR Responding Gateway does not properly detect a SOAP header XML Digital Signature discrepancy.

Mitigation: The PHR vendor will have periodic unannounced security assessments by Sequoia Project eHealth Exchange Support Staff, or a designated Sequoia Project contractor.

Threat: Other threats enumerated in the eHealth Exchange Security Assessment document.

Mitigation: PHR vendor will review the assessment and mitigate any applicable risks.

Threat: PHR Responding Gateway does implement 2-way-TLS mutual authentication properly.

Mitigation: The PHR vendor will have periodic unannounced security assessments by Sequoia Project eHealth Exchange Support Staff, or a designated Sequoia Project contractor.

[Reviewers: Please provide additional threats you feel we should document.]

Operational Considerations

Service Levels

CONF#### PHR Responding Gateways (and ACP Responding Gateways) MUST respond to requests within 10 seconds. Specifically, the amount of time measured will be measured from the time a request is received by the PHR eHealth Exchange Responding gateway service, until the response from that gateway. The sum of the response time from all three of the eHealth Exchange Patient Discovery (PD), Query for Documents (QD) and Retrieve Documents (RD) must be less than 10 seconds total. For example, if the PHR Responding Gateway takes 2 seconds to respond to a PD request, and 2 seconds to respond to a QD request, then it must respond to the RD request in 6 seconds or less.

CONF#### The availability of the PHR service must exceed 99.9%, less scheduled maintenance activities.

Operational Monitoring

[Reviewers: We anticipate proposing a new OP&P #10 that would allow eHealth Exchange Support Staff to implement a technical operational monitoring service to periodically assess conformance to this service level using a mutually agreed upon test Patient.]

Validation Environment

The PHR implementer will maintain an operational validation environment which is physically distinct from their production environment. The validation environment is not expected to have the same availability, response times, or capacity as the production environment. But it is expected to provide a well-maintained environment to facilitate partner testing.

Reports

Service levels (response times and availability) will be published publically.

Validation Plan

[Reviewers: This section is expected to will probably be moved to a new document. All statements in this document that are normative requirements are denoted by a CONF prefix. Each of these conformance statements will be gathered in the final version of the PHR Profile document, in the Validation Plan section, and will become part of an approved eHealth Exchange Validation Plan. The below list is incomplete.]

CONF#### PHR Implementer MUST deploy a system that has passed the applicable sections of the PHR Profile Validation Plan.

CONF #### PHR Implementer MUST deploy a validation environment that complies with the eHealth Exchange Performance and Service Specifications, including the PHR Profile.

CONF #### PHR Implementer MUST deploy a production environment that complies with the eHealth Exchange Performance and Service Specifications, including the PHR Profile.

CONF #### PHR Implementers acting as Initiators MUST successfully pass the existing eHealth Exchange Validation Program requirements for Initiating Gateways.

CONF #### PHR Implementers acting as Initiators MUST successfully pass the existing eHealth Exchange Validation Program requirements for Access Consent Policy Initiating Gateways.

CONF #### PHR Implementers acting as Responders MUST successfully pass the existing eHealth Exchange Validation Program requirements for Responding Gateways.

FAQ

Q: What is the difference between a Patient and an End-User?

A: A Patient is the subject of a given clinical data set. For example, a laboratory results message is associated with the Patient. An End-User is a person authorized to log in (authenticate) to the PHR software. An End-User may be the Patient. An End-User may also be authorized in some circumstances to view and manage clinical data in the PHR for others such as minor children. See also Definitions.

Q: How would medical proxies be able to use a PHR, such as, for example, a parent managing the health record of a minor child?

A: Implementers of the PHR Profile in production under the eHealth Exchange must be participants to the DURSA legal agreement which states the following “Uses and disclosures pursuant to an Authorization provided by the individual who is the subject of the Message or such individual’s personal representative as described in 45 C.F.R. § 164.502(g) of the HIPAA Regulations.”

Q: Will a Patient be able to search for data for other Patients?

A: End-Users are those that are provisioned and log in (authenticate) to the PHR implementation. End-Users are not allowed to change their demographic traits. Demographic traits can only be changed by trusted staff at PHR vendor implementations, and must be identity proofed to NIST 800-63-2 level 3 or 4. As a result, End-Users can only search for data based on immutable traits for themselves or for those they are specifically authorized for. See Patient Matching.

Q: Can a medical proxy disambiguate the Patient since they are more trusted? In other words, can a specific End-User of the PHR be used to perform an ambiguous search and then to select the correct Patient record?

A: No. PHR End-Users cannot be presented with a list of multiple Patient records. However, PHR Vendor staff may perform this function during the End-User provisioning process.

[Note: Please include additional questions and/or answers here that you think will be common for this profile.]

Appendix A: Coordinating Committee Issue Brief

[Reviewers: The eHealth Exchange CC approved the following document, at a conceptual level. It is included for reference during the profile development and will likely be removed for the final version of the profile.]

Issue Brief

Date: 9/9/15

Topic: Personal Health Record (PHR) Profile

Background: Several organizations that wish to offer PHR services expressed interest in joining the eHealth Exchange to enable individuals to query for their own health records. Based on this interest, the Coordinating Committee approved moving forward with a pilot, which included the development of a PHR profile that details the technical requirements for PHRs that want to onboard to the eHealth Exchange.

In the case of a PHR network that offers its service via employer health plans, the employer health plan wants to enable beneficiaries to query for their own health records to better manage their own care. The PHR is populated with eligibility and demographic data from the plan and the PHR network obtains an individual's authorization prior to enabling an individuals to request their own records.

Technical Due Diligence: The eHealth Exchange Support Staff conducted due diligence to understand the architecture, security controls and function of PHR systems, which were documented in a requirements document. Additional due diligence will be conducted by the Specification Factory and Testing Work Groups.

Policy Due Diligence: Troutman Sanders completed analysis to assess whether PHR vendors, PHR networks or employer-sponsored health plans satisfy the eligibility criteria and the permitted purposes in the DURSA and determined the following:

a. A PHR network would likely have the structure and authority to meet the eligibility requirements, specifically the requirement that a Participant be an organization that oversees and conducts, on its own behalf and/or on behalf of its Participant Users, electronic transactions or exchanges of health information among groups of persons or organizations. Similarly, if the PHR is tethered to an employer-sponsored health plan, it is likely to have the attributes related to overseeing and conducting electronic transactions of health information. A PHR that serves solely as a technology vendor might not have these required attributes.
b. To be an eligible Participant, an organization must be prepared to engage in the exchange of information for a Permitted Purpose as defined in the DURSA. The permitted purpose related to Authorization would satisfy this. "Uses and disclosures pursuant to an Authorization provided by the individual who is the subject of the

Message or such individual's personal representative as described in 45 C.F.R. § 164.502(g) of the HIPAA Regulations."

Applicants who are approved by the Coordinating Committee to support the PHR Profile shall satisfy the following General Eligibility Criteria and Technical Requirements as detailed in Operating Policy and Procedure #1 (OPP#1) (reproduced below for your reference):

General Eligibility Requirements (Administrative)

a. Be a valid business in good standing or a governmental agency, operating in the United States;
b. Meet all solvency and financial responsibility requirements imposed on the Applicant by applicable statutes and regulatory authorities;
c. Be an organization or agency that oversees and conducts, on its own behalf and/or on behalf of its Participant Users, electronic transactions or exchanges of health information among groups of persons or organizations;
d. Utilize a system which has been verified as compliant with the Performance and Service Specifications;
e. Have the organizational infrastructure and legal authority (through statutes, regulations, organizational agreements, contracts or binding policies) to comply with the obligations in the DURSA and to require its Participant Users to comply with applicable requirements of the DURSA;
f. Intend to Transact information with other Participants for a Permitted Purpose;
g. Have sufficient financial, technical and operational resources to support the testing and operation of transactions among Participants;
h. Is not aware of any information that would preclude the Applicant from fully complying with the provisions of the DURSA; and
i. Submit the completed Application, the signed DURSA Joinder Agreement (Attachment 7 of the DURSA), and the eHealth Exchange Participation Agreement along with the applicable participation fees.

Technical Requirements

a. Has a system implemented in a production-ready environment that complies with the Performance and Service Specifications;
b. Successfully complete the required technical testing of Applicant's system in accordance with the Validation Plan; and
c. Certify the Applicant is ready to begin exchanging data with other eHealth Exchange Participants in production through the Applicant's successfully tested system.

Below are additional proposed new requirements for PHRs. We are proposing that these new requirements will be placed into a new PHR profile which will become a new addendum to the Performance and Service Specifications.

Additional Requirements for PHR Profile

a. The PHR shall obtain a HIPAA compliant authorization from the End-User, and import personal health information from a data source into an End-User's record

b. The End-User shall be identity proofed to the applicable version of the NIST 800-63 publication series, level 3 or above (e.g. an employee that has a background check and I-9 verification of employment eligibility.)

c. The PHR shall permit query for documents only on behalf of registered End-Users and solely for the benefit of the End-User as per the DURSA Permitted Purposes clause. (For your reference, this clause states "Uses and disclosures pursuant to an Authorization provided by the individual who is the subject of the Message or such individual's personal representative as described in 45 C.F.R. § 164.502(g) of the HIPAA Regulations.")

d. The PHR shall not use the eHealth Exchange to perform a query for any data other than as allowed by the DURSA Permitted Purposes clause.

e. The PHR shall implement technical controls to minimize the likelihood of an End-User from obtaining information other than their own (e.g. In the event of a hospital records error or similar event where a Patient was incorrectly linked or incorrectly merged, a Patient may receive the wrong information).

f. The PHR will make the Patient trait criteria used for matching immutable (i.e., should birth date be used for matching logic, the End-User shall not be able to change birth date to a different value and re-query for documents.) In addition, the PHR will agree on the Patient matching logic to minimize the possibility of ambiguous matches. (e.g. the PHR will match on traits such as an identifier).

g. Outbound eHealth Exchange queries from the PHR shall use the Purpose of Use and Role codes indicating that the request is being made pursuant to a Patient authorization and that the request is being made on behalf of the Patient. The PurposeOfUse value shall be 'REQUEST' as per the eHealth Exchange Authorization Framework Specification v3.0 http://sequoiaproject.org/wp-content/uploads/2014/11/nhin-authorization-framework-production-specification-v3.0.pdf table 3.3.2.6-1 and it is defined as the individual (pursuant to authorization). The Role code shall be "116154003" with a displayname of "Patient" as per the NWHIN Authorization Framework Specification v30, as per HITSP C80 Table 2-155 with a value set OID of 2.16.840.1.113883.3.18.6.1.15. In version 2.0 of the Authorization Framework Specification http://sequoiaproject.org/wp-content/uploads/2014/11/nhin-authorization-framework-production-specification-v2.0.pdf in table 4

h. The PHR shall respond to all inbound requests within 10 seconds.

Appendix B – Outstanding Issues

[Reviewers: The items in this list will be addressed as directed by eHealth Exchange Participants. Please very carefully review and indicate which of these items, if any, need to be included in the first trial implementation version of the PHR Profile. Also, please indicate any ADDITIONAL items that need to be in the first trial implementation of the PHR Profile.]

Additional Use Cases

1. A PHR deployment allows for Patients to provide self-entered data into the PHR with the anticipation of sharing it with one or more authorized eHealth Exchange Participants.
2. A Patient changes clinicians or organizational affiliations.
3. A PHR data source or affiliation merges, unmerges, etc.
4. Patient uses a robust provider directory to identify sources of exchange.
5. A Patient self-enrolls into a PHR
   - Patient correlation (out of band vs. in response to a Patient Discovery request)
   - A Publish subscribe message exchange pattern

Potential Sub Use Cases

- Tethered PHRs vs Untethered
- Tethered PHR Moves Affiliation
- Secure Email – broader than Direct Project emails
- FHIR based interoperability

Other Pending Issues

- Minors/dependents/non-ID proofed individuals
  - How would this be represented in the authorization?
- Should this profile have a conformance statement regarding support for the effective date range, specific attributes such as for specific types of data
- Is there an existing architecture where a PHR queries an exchange? One state HIE attempted a state-wide Patient portal (didn't go live) but was similar where a Patient could select the data sources. This architecture can present some new and specific security threats and opportunities.
- Can/should we decouple PD from QD and RD since there is different risk for PD? Such as having a system admin do PD and then allow the Patient to do QD and RD?
- Will a Patient be able to query often enough to cause a performance problem with responding systems? Systems should have technical controls in place to prevent this.

[Reviewers: As mentioned above, please provide feedback on the above issues to help determine which issues must be addressed in the first PHR Profile for trial implementation.]