eHealth Exchange

Operating Policy and Procedure

| SUBJECT: EHEALTH EXCHANGE SERVICE LEVELS AND OPERATIONAL MONITORING | | |
|---|---|---|
| **Status: Final – Approved by CC** | **Policy #: OPP-11** | |
| **Effective Date: 6/19/2016** | **Version: v1.0** | **Page 1 of 6** |

## *I. Purpose*

The eHealth Exchange currently operates as a federated network with no centralized mechanism to capture metrics or to provide quality assurance about Participant system availability, performance, content quality, conformance, etc. This type of operational monitoring is important for the eHealth Exchange network to assist Participants in proactively identifying issues and in developing strategies and solutions to minimize system timeouts and unpredictable response times.

Participants are obligated, in Section 15.08 of the DURSA, to transmit information to other Participants in a timely manner. The eHealth Exchange Coordinating Committee is establishing a process to monitor Participant's system performance to improve the reliability and responsiveness of the transmissions across the eHealth Exchange network. To that end, the Coordinating Committee delegates responsibility to Healtheway, Inc. (d/b/a The Sequoia Project, "Sequoia") and its eHealth Exchange Support Staff ("Staff"), to provide operational support to eHealth Exchange Participants and the Coordinating Committee, including but not limited to the set of responsibilities outlined in OPP #1 and OPP #9 as well as facilitating the operational monitoring necessary to implement OPP #11, described below.

The purpose of this OPP is to capture key operational metrics including, but not limited to, reachability, availability and response time. These metrics will be provided to the Coordinating Committee to aid their determination of the need for, and nature of, any future requirements related to eHealth Exchange Service Levels. The system will be designed with technical controls to prevent PHI from being exchanged during the monitoring process and thus Sequoia will not become a Business Associate of Participants as a result of such monitoring.

## *II. Policy*

Staff will monitor the performance of all Participants' gateways in the PRODUCTION environment. Monitoring may also be conducted in the VALIDATION environment. Monitoring will be conducted on a schedule as defined in section IV. The results of assessments will be aggregated across Participants and published to designated contacts at each Participant and to the Coordinating Committee. The report will include aggregated performance data, plus identifiable performance results only for that specific Participant. PRODUCTION monitoring will be maintained

separately from VALIDATION monitoring. Any data provided to Participants about other Participants will be de-identified. The operational monitoring system will be designed to have technical enforcement to prevent Protected Health Information from being accessed, and thus Sequoia will not become a Business Associate due to this assessment. The operational monitoring system source code will be available to inspection by designated staff at Participants to help ensure transparency, and protection of PHI, in the operational monitoring process.

## *III. Procedure:*

1. Staff will run an operational monitoring system designed to determine certain information about each Participant gateway.
2. Staff will provide Participants with a scorecard that reports, at a minimum, the following metrics on a periodic basis:
    a. Reachability – Determine if communications are possible with the gateway.
    b. Availability – Determine if the gateway service is up and running.
    c. Response Time – Determine the speed at which a gateway replies to test transactions.
3. Phase I collected data will include the date and time of the monitoring assessments, name of the Participants, IP addresses, domain names, port numbers, service end points, response codes, test types, and the response times. For Phase II, collected data will be expanded to include number of test patients matched, number of test documents retrieved and sizes of test documents retrieved.
4. Staff will analyze the collected data and publish it in aggregated format to inform the Coordinating Committee on a monthly basis.
5. Staff will review the performance metrics of each Participant, and provide a report to each Participant with that Participant's metrics on a monthly basis. Staff will also provide an aggregated report of other Participants' metrics to each Participant.
6. To help eliminate the possibility of PHI from being accessed by Staff, all tests will be structured to use parameters designed to return no actual patient data. This

will implemented by using demographics that are known to be associated only with test patients and/or demographics that are known to not correlate to any patient, such an invalid patient ID, and via specific technical values in the request, as documented in Section IV immediately below.

## *IV. Approach:*

1. SAML attributes as populated by the operational monitoring system:
    a. Home Community ID: urn:oid:1
    b. Patient ID assigning authority and patient ID (resource-id): 0/0 or a mutually agreed upon test patient ID
    c. Issuer: CN=OPERATIONS.SEQUOIAPROJECT.ORG,OU=NHIN,O=HHS-ONC,C=US
    d. Subject: admin@sequoiaproject.org
    e. Subject ID: Sequoia Operational Monitoring System
    f. Subject Organization: The Sequoia Project
    g. Subject Organization ID: http://operations.sequoiaproject.org
    h. Subject Role: IT Professional
    i. Purpose Of Use: OPERATIONS
        i. OPERATIONS was selected as it is expected that most Participants would reject messages with this PurposeOfUse until explicitly allowed.
        ii. An intentional result of this behavior is that access to PHI is expected to be declined until the Participant confirms it has technical enforcement in place to prevent access to PHI.
    j. Resource ID: 1
2. Messages tested:
    a. Phase I
        i. Initially only low-level transactions, such as ICMP (Ping), 2-way-TLS and HTTP, and Patient Discovery messages will be transacted with each Participant gateway, using query parameters that are known to result in an unsuccessful query.
    b. Phase II
        i. Once a test patient is identified at that Participant, and once that Participant confirms it can technically enforce responses to ensure they only contain test patients, then the operational monitoring system will transmit Patient Discovery messages using test patient query parameters, with subsequent Query for Documents and Retrieve Documents messages for such test patients. The ability of the

operational monitoring system to query a configurable test patient is intended to minimize Participant burden.

c. Test patients would be mutually determined between Staff and each Participant.
d. Staff will help ensure that the test patient data is normalized, especially in terms of message sizes.

3. Security considerations:
   a. Within the context of operational monitoring, Participants should configure their systems to only respond to queries from the operational monitoring system with test patients. The various attributes defined in section IV are designed to enable Participants to accommodate this objective via various filtering and access control mechanisms in a vendor-neutral manner.
   b. Until each Participant confirms that it has enacted technical enforcement to ensure only test patient data is returned in response to queries, the operational monitoring system will only submit requests which return no patient responses.
4. Responder gateway monitoring:
   a. The initial scope of this OPP is to only monitor responding gateways. In the future, initiating gateways may be within scope, under a revised OPP#11.
5. PRODUCTION vs. VALIDATION gateway operational monitoring:
   a. PRODUCTION will be assessed against at least three criteria, reachability, availability, and response time. The VALIDATION environment will be accessed at the discretion of Staff and will likely included more limited tests, such as reachability and availability.
6. Validation of the operational monitoring system:
   a. The operational monitoring system will be validated via a three (3) month pilot, measured from the time the operational monitoring system begins operation. The results of the pilot will be presented to the Coordinating Committee so that they may determine if the pilot should continue into full production status, or take some other action. If the Coordinating Committee takes no explicit action, then production operational monitoring will begin after the pilot is completed.
   b. The pilot deployment will perform operational monitoring of all eHealth Exchange Participants that are in production.
   c. The operational monitoring system would not require any changes to the eHealth Exchange Validation Program.
   d. For Phase I the operational monitoring system will use parameters, as defined in this section, design to elicit error responses from Participant systems and thus will not be tested under the eHealth Exchange Validation

Program as the operational monitoring system intentionally will be unable to initiate a successful query. Phase II queries will be assessed using the Validation Program.

7. Scheduled downtime considerations:
    a. Evaluation of systems will be adjusted for systems during pre-scheduled down time windows, provided notification of such a down time window was supplied to, and automatically acknowledged by, techsupport@sequiaproject.com, at least three (3) business days in advance of the beginning of the down time. Metrics will reflect scheduled down times (as well as unscheduled down times).
8. Report format:
    a. The report will contain at least the following values: date and time range of the assessments, reachability status, availability status, and response time metrics (for the PRODUCTION environment). VALIDATION reports will not initially contain performance metrics.
    b. Times in the report would be time adjusted to UTC.
9. Frequency of monitoring:
    a. Operational monitoring assessments will be conducted approximately once per hour, per participant, 24x7x365 during the pilot. If adjustment to this assessment frequency is indicated by pilot participants then the Coordinating Committee will be apprised of such feedback so they may consider an altered frequency of monitoring.
10. Code review:
    a. Designated technical staff at Participant organizations will be able to review the operational monitoring system source code.
11. Participant metrics considerations:
    a. The service monitoring system may impact Participant operational reports. Thus the operational monitoring system will use SAML and query parameter attributes as defined in Section IV to allow Participants to implement compensating capabilities.
12. The certificate presented by the operational monitoring system will use the following attributes:
    a. Chain of trust: The operational monitoring system will employ the same chain of trust as eHealth Exchange PRODUCTION certificates for PRODUCTION operational monitoring, and VALIDATION certificates for any VALIDATION operational monitoring.
    b. End Entity certificate: Subject DN: CN=OPERATIONS.SEQUOIAPROJECT.ORG, OU=NHIN, O=HHS-ONC, C=US

## *V. Definitions:*

**DURSA** – Data Use and Reciprocal Support Agreement

Additional definitions to be added

All other capitalized terms, if not defined herein, shall have the same meaning as set forth in the DURSA.

## *V. References:*

- DURSA, Section 14
- DURSA, Section 15
- DURSA, Section 17.01
- DURSA, Section 19
- eHealth Exchange Issue Resolution Process

## *VI. Related Policies and Procedures:*

- OPP #1: Participation – Review and Disposition of Applications for Participation
- OPP #3: Participation – Changes, Suspension, Termination
- OPP #9: eHealth Exchange Digital Credentials

## *VII. Version History:*

| ID | Date | Author | Status | Comment |
|---|---|---|---|---|
| *1* | 5/17/2016 | Jennifer Rosas/Eric Heflin | Published | First eHealth Exchange Coordinating Committee approved version. |