eHealth Exchange

Operating Policy and Procedure

SUBJECT: EHEALTH EXCHANGE DIGITAL CREDENTIALS		
Status: FINAL – Approved by CC	**Policy #: OPP-9**	
Effective Date: 3/11/16	**Version: Final v2**	**Page 1 of 4**

I. Purpose

eHealth Exchange digital certificates, are issued, managed, held and revoked in accordance with the DURSA and Federal Bridge Certificate Authority (FBCA) policy, under the authority of the eHealth Exchange Coordinating Committee (Coordinating Committee). These certificates serve as the "Digital Credentials" referenced in the DURSA and are used by eHealth Exchange Participants to authenticate to each other prior to the transmission of Message Content, to encrypt the communications channel for the exchange of Message Content, and to digitally sign certain components of the Message Content.

eHealth Exchange Digital Credentials are only intended to be used to exchange Message Content between eHealth Exchange Participants, as governed by the DURSA and Coordinating Committee. This OP&P clarifies several deployment options.

Use of Digital Credentials for other purposes or for exchanging data with organizations who are not eHealth Exchange Participants, increases risk to those Participants. For example, use of Digital Credentials for other uses creates a dependency, putting other uses and applications at risk since the Digital Credentials may be revoked, held, or re-issued in accordance with the DURSA, FBCA and Coordinating Committee.

II. Policy

1. While it is discouraged, eHealth Exchange Participants may, at their own risk, utilize eHealth Exchange Digital Credentials (which are x.509 digital certificates) for purposes other than to secure eHealth Exchange gateway 2-way-TLS connections and signing components of eHealth Exchange transacted messages, with the following conditions:
    a. Signed public certificate and private key may only be used to facilitate the security of messages transacted for healthcare-related purposes and/or DURSA Permitted Purposes.
    b. Signed public certificate and private key may only be used to secure only SOAP or REST based transport or for digital signatures creation or validation.
    c. Private keys may only be installed in a Secure Environment, and must never be duplicated outside of that Secure Environment or shared in any way.
    d. Private keys may only be installed in a Secure Environment that is also acting as the eHealth Exchange Participant gateway.

    eHealth Exchange Participants may:
    a. Install the eHealth Exchange root certificate on any server.
    b. Install the eHealth Exchange intermediate certificate on any server.
    c. Install the eHealth Exchange public key and signed server certificate on any server.

    These other uses would not be supported by eHealth Exchange or governed by the Coordinating Committee; however, the eHealth Exchange certificate support processes would still apply.

Organizations incur risk of a certificate being revoked, held, or re-issued at any time and could thus experience unexpected operational outages for systems using eHealth Exchange x.509 certificates for other purposes.

2. Configure their Secure Environment to only allow eHealth Exchange Participant access

   Participants must configure their eHealth Exchange gateway to only accept inbound requests from other eHealth Exchange Participants, other than as allowed in section II(1) above. Configuration of each environment is unique, and thus eHealth Exchange Support Staff are unable to provide authoritative and complete configuration requirements. However, Participants must meet the following requirements, at a minimum, and with the exceptions as permitted in II(1) above:
   a. Require their Subscriber and security staff to read, review, and attest they have mitigated each risk defined in the current version of the eHealth Exchange Security Assessment. This attestation will be required each time a Participant x.509 certificate is issued or re-issued.
   b. Have implemented x.509 certificate filtering to prevent non-eHealth Exchange certificates from being accepted at the 2-way-TLS layer.
   c. Have implemented x.509 certificate revocation checking to prevent "held", or "revoked" eHealth Exchange certificates from being accepted at the 2-way-TLS layer.
   d. Have implemented x.509 certificate revocation checking to prevent expired, corrupted, or other invalid eHealth Exchange certificates from being accepted at the 2-way-TLS layer.
   e. Have implemented their PRODUCTION Secure Environment so that it does not accept eHealth Exchange VALIDATION certificates, and vice versa.
   f. Allow a monthly, limited scope, security test by eHealth Exchange Support Staff. This test will utilize technical controls designed to prevent Protected Health Information ("PHI") from being accessed during the test, such controls to be open to inspection by Participants' Subscribers. THIS SECURITY TEST IS NOT A REPRESENTATION BY THE eHEALTH EXCHANGE COORDINATING COMMITTEE OR ITS DESIGNEEE OF PROPER SECURITY CONFIGURATION, nor is it a substitute for a Participant security audit. In the event a deficiency is identified, it will be treated as a business confidential/need to know only disclosure, and eHealth Exchange Support Staff will work privately with Participant to remediate such identified defects using Information Security "Responsible Disclosure" guidelines.

III. Procedure:

Delegation of Rights

The Coordinating Committee has designated Healtheway, Inc. (d/b/a/ The Sequoia Project, "Sequoia") and its staff ("eHealth Exchange Support 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. In addition, the Coordinating Committee has delegated responsibility to Sequoia and its eHealth Exchange Support Staff to facilitate the security testing necessary to implement the policies in OPP #9 described

above.

IV. Definitions:

DURSA: Data Use and Reciprocal Support Agreement

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

Responsible Disclosure – A practice developed by the Information Security community to ensure that identified vulnerabilities in security-related systems are resolved in a manner that protects the privacy and operational integrity of impacted systems until the vulnerability is remediated. A key component of this process is to only provide the vulnerability information on a need to know basis.

REST – An acronym for Representational State Transfer which is a method of information exchange that uses a web-browser-like approach to contact message content. This method is used by the HL7 FHIR® standard.

Secure Environment – In the context of this OP&P, a secure environment is defined as a single computer, in a data center with appropriate physical and software access controls to prevent inappropriate access by unauthorized people or systems. A secure environment also optionally includes a high availability cluster of computers designed to mimic the cryptographic behavior of a single system, and it also includes a disaster response data center operated to closely mimic the behavior of the primary data center.

SOAP – A method of transacting message content exchange using XML. This method is uused by the eHealth Exchange Patient Discovery, Messaging Platform, Access Consent Policies, and other specifications.

Subscriber – The single named individual employed by the Participant responsible for overseeing the following: obtaining, installing, and securely managing the eHealth Exchange x.509 certificate and the associated Secure Environment. The Subscriber must be able to enter into binding legal agreements on behalf of the Participant, and must have sufficient technical and security knowledge in order to manage the eHealth Exchange x.509 certificate securely. The Subscriber is typically a CIO, CTO, Director of IT, or similar individual.

V. References:

- DURSA, Section 14
- DURSA, Section 17.01
- DURSA, Section 19

VI. Related Policies and Procedures:

- ***OPP #1: Participation – Review and Disposition of Applications for Participation***
- OPP #3: Participation – Changes, Suspension, Termination

VII. Version History:

ID	Date	Author	Comment
1	3/27/14	Eric Heflin / Specifications Factory	Drafted policy, based upon recommendations from Policy & Technical Task Group
2	4/1/14	Jennifer Rosas	Minor editorial revisions
3	4/1/14	Jennifer Rosas	Minor editorial revisions
4	7/20/15	*Kati Odom*	Revised to reflect Healtheway name change to Sequoia Project
5	1/10/16	*Eric Heflin*	Added section #3, additional definitions, plus a certificate "hold" status text
6	1/11/16	*Gonzalo Hernando*	Additional clarifications related to testing and Subscriber responsibilities
7	1/15/16	*Jennifer Rosas, Mariann Yeager, Eric Heflin*	Additional text related to the DURSA, new definitions, and clarifications on delegated responsibility.