eHealth Exchange

Operating Policy and Procedure

SUBJECT: EHEALTH EXCHANGE DIGITAL CREDENTIALS		
Status: FINAL – Approved by CC	**Policy #: OPP-9**	
Effective Date: 5/5/14	**Version: Final**	**Page 1 of 4**

I. Purpose

eHealth Exchange digital certificates, are issued, managed 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 and to digitally sign certain components of the SOAP messages.

eHealth Exchange Digital Credentials are only intended to be used to exchange Message Content only with other eHealth Exchange Participants, as governed by the DURSA and Coordinating Committee.

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

II. Policy

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:

1. 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.
2. Signed public certificate and private key may only be used to secure only SOAP based transport or for digital signatures creation or validation.
3. Private keys may only be installed on only a single server or high availability cluster, and must never be duplicated outside of that server or cluster or shared in any way.
4. Private keys may only be installed on only a single server, or high availability cluster, that is also acting as the eHealth Exchange Participant gateway.

eHealth Exchange Participants may:

1. Install the Entrust root certificate on any server.
2. Install the eHealth Exchange public key and signed certificate on any server.

These other uses would not be supported by Healtheway or governed by the Coordinating Committee; however, the Healtheway certificate support processes would still apply. Organizations incur risk of a certificate being revoked or re-issued at any time and could thus experience unexpected operational outages for systems using eHealth Exchange x.509 certificates for other purposes.

III. Procedure: *N/A*

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.

V. References:

- DURSA, Section 17.01
- DURSA, Section 19

VI. Related Policies and Procedures:

- OPP #3: Participation – Changes, Suspension, Termination

VII. Version History:

	Date	Author	Comment
1	3/27/14	Specifications Factory	Drafted policy, based upon recommendations from Policy & Technical Task Group
2	4/1/14	J. Rosas	Minor editorial revisions