ClinicalConnect
Health Information Exchange

TITLE: DIGITAL CERTIFICATE POLICY	
STATUS: FINAL	**EFFECTIVE DATE: March 24, 2015**
VERSION: 7	**PAGE: 1 OF 3**

I. PURPOSE

It is the policy of ClinicalConnect Health Information Exchange (CCHIE) to ensure secure measures are followed when handling digital certificates and to comply with any applicable state and federal law and regulations, and/or digital credential requirements established by the eHealth Exchange.

II. SCOPE

This policy applies to ClinicalConnect HIE staff members and it's service provider.

III. DEFINITIONS

"Digital certificates" - also known as digital credentials or x.509 certificates - are utilized to securely exchange data over the internet and to confirm and verify the identity of each exchange party. Digital Certificates are issued by a Certificate-Issuing Authority ("CA") and as such a recipient can verify that the certificate is real and issued by an official trusted agency. A certificate contains the name of the certificate holder, a serial number, expiration dates, and a copy of the certificate holder's public key which is used for encrypting messages and digital signatures.

"DURSA", Data Use and Reciprocal Support Agreement is a comprehensive, legal multi-party trust agreement that is entered into voluntarily by public and private organizations (eHealth Exchange Participants) that desire to engage in electronic health information exchange with each other as part of the eHealth Exchange.

"eHealth Exchange", formerly known as the *Nationwide Health Information Network* and often abbreviated as the *NHIN* or *NwHIN*, shall mean a group of organizations with a common mission and purpose to improve patient care, streamline disability benefit claims, and improve public health reporting through secure, trusted, and interoperable health information exchange.

"Participant" is an organization (including physician practice) that has signed a Data Exchange Agreement with the ClinicalConnect HIE.

"PA Patient and Provider Network" also known as "P3N," is the network that supports the ability of healthcare participants to exchange information within and beyond Pennsylvania's borders.

"Service Provider" is an organization that has signed a support agreement with the ClinicalConnect HIE to provide technology related services necessary to operate the health information exchange.

IV. POLICY

A. ClinicalConnect HIE and its service providers shall adhere to and/or follow x.509 key management best practices, applicable law, and FBCA procedures and policies.

B. Digital certificates, keys, and/or passwords issued to ClinicalConnect HIE shall be used for ClinicalConnect HIE business transactions only.

C. ClinicalConnect HIE, its service providers, participant organizations, users, certificate subscribers and/or proxy shall not disclose any keys, passwords, certificates, or any other security measures that enable connectivity.

D. ClinicalConnect HIE and its service providers shall ensure that digital certificates and/or keys shall never leave the server it is intended for and shall be stored and/or deployed by trusted staff in a secure environment.

E. ClinicalConnect HIE and its service providers shall ensure that digital certificates are managed and revoked per eHealth Exchange and P3N certificate policies and procedures.

F. eHealth Exchange digital certificates are issued, managed and revoked in accordance with The Sequoia Project Data Use and Reciprocal Support Agreement (DURSA) and Federal Bridge Certificate Authority (FBCA) policy, under the authority of the eHealth Exchange Coordinating Committee. These certificates serve as the Digital Credentials referenced in eHealth Exchange DURSA.

G. eHealth Exchange digital credentials shall only be utilized for purposes of eHealth Exchange transacted messages and/or for the security of messages transacted for healthcare related purposes and/or DURSA Permitted Purposes.

H. eHealth Exchange validation (test) digital certificates shall be created and reside on a validation server that contains test data only.

I. eHealth Exchange production digital certificates shall be created and reside on the production server only.

J. eHealth Exchange validation (test) digital certificates and production digital certificates shall be renewed yearly per eHealth Exchange Certificate Authority (CA).

K. Upon being reasonably aware or suspected, ClinicalConnect HIE support and management shall be notified promptly of the compromise of digital certificates, keys, and/or passwords.

1. For compromised eHealth Exchange digital certificates, ClinicalConnect HIE and/or its service provider shall notify and revoke per eHealth Exchange techsupport@ehealthexchange.org and the P3N/technology vendor (http://truvenhealth.com/support/portal/) policies and procedures.

V. Revision History

DATE	AUTHOR	COMMENTS
03/24/2015	Dianne Clark	Creation of the Policy
12/24/2015	Erika Jones	Updated the template
02/13/2017	Dianne Clark	Reviewed/updated details
02/20/2017	Dianne Clark	Added revoke notation for compromised certificates
06/30/2020	Brandon Lyons	Updated Sequoia Project with eHealth Exchange and support email
01/07/2022	Keith Dukes	Adjusted title and re-formatted dates.
6/10/2022	Mike Gigliotti	FY22 Policy Review: No updates.