ClinicalConnect
Health Information Exchange

TITLE: DATA BREACH NOTIFICATION POLICY	
STATUS: FINAL	**EFFECTIVE DATE: September 9, 2015**
VERSION: 5	**PAGE: 1 OF 4**

I. PURPOSE

This policy sets forth the minimum standards the ClinicalConnect HIE (CCHIE) and its Participants shall follow in the event there is a breach of unsecured Protected Health Information (PHI) in a manner not permitted under the Health Insurance Portability and Accountability Act of 1996 and its implementing rules and regulations, which comprise the security or privacy of the PHI.

II. OVERVIEW

This policy outlines an action plan that will be used to investigate potential breaches and to mitigate damage if a suspected Breach occurs. This policy is in place to both minimize potential damages that could result from a Breach and to ensure that parties affected by a Breach are properly informed as to how to protect themselves.

III. SCOPE

This policy is for CCHIE employees and its Participants.

IV. DEFINITIONS

"Breach" shall have the same meaning and include the requirements set forth at 45 CFR § 164.508 of the HIPAA regulations and include any similar but additional requirements under Applicable Law.

"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.

"Health Data" shall mean that information which is requested, disclosed, stored on, made available on, or sent by or to Provider or an HIE Participant through the HIE. This includes, but is not limited to, Protected Health Information (PHI), individually identifiable information, de-identified data (as defined in the HIPAA Regulations), Limited Data Sets, pseudonymized data, metadata, and schema.

"Message Content" shall mean that information contained within a Message or accompanying a Message using the Specifications. This information includes, but is not limited to, Protected Health Information (PHI), de-identified data (as defined in the HIPAA Regulations at 45 C.F.R. § 164.514), individually identifiable information, pseudonymized data, metadata, Digital Credentials, and schema.

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

"Protected Health Information" or "PHI" shall have the same meaning as set forth in HIPAA.

V. GUIDELINES FOR BREACH NOTIFICATION BY CCHIE PARTICIPANTS

A. Within one (1) hour of discovering information that causes reasonable belief that a breach may have occurred, a Participant shall report a suspected Breach to CCHIE and other CCHIE Participants whose Health Data may have been Breached.

B. As soon as reasonably practicable, but no later than twenty-four (24) hours after determining that a Breach occurred, a Participant shall notify CCHIE and all CCHIE Participants likely impacted by the Breach of such Breach. The notification shall include sufficient information for the CCHIE and Participants to understand the nature of the Breach. For instance, such notification could include, to the extent available at the time of the notification, the following information:

1. Description of the Breach
2. Description of the roles of the people involved in the Breach (e.g. employees, users, service providers, unauthorized persons, etc.)
3. The type of health data Breached
4. CCHIE Participants likely impacted by Breach
5. Number of individuals or records impacted/estimated to be impacted by the Breach
6. Actions taken by the Participant to mitigate the Breach
7. Corrective action taken and steps planned to be taken to prevent a similar Breach

C. The Participant shall supplement the information contained in the Breach notification as it becomes available and cooperate with other Participants and CCHIE in performing such actions as are required and necessary to mitigate the harmful effect of the Breach.

D. CCHIE Security and Compliance Analyst shall name an individual to act as the investigator of the Breach. The investigator shall be responsible for the management of the Breach investigation and coordinating with others as appropriate. The investigator shall be the key facilitator for all breach notification processes.

E. CCHIE shall conduct a thorough risk assessment to determine the extent of the Breach and document the risk assessment as well as the outcome of the process.

F. If, on the basis of the Breach information, CCHIE determines that (i) the other CCHIE Participants that have not been notified of the Breach would benefit from a summary of the notification or (ii) a summary of the notification to the other Participants would enhance the security of CCHIE or the Participants' environment, CCHIE may provide, in a timely manner, a summary to such CCHIE Participants that does not identify any of the Participants or individuals involved in the Breach.

G. The Participant, CCHIE and the affected Participants shall decide on a case-by-case basis which party should notify any affected patients, and other parties as required by law.

VI. GUIDELINES FOR BREACH NOTIFICATION TO PARTICIPANTS, eHEALTH EXCHANGE, and P3N

A. Within one (1) hour of discovering information that causes reasonable belief that a breach may have occurred, CCHIE shall alert The Sequoia Project ("Coordinating Committee") (admin@sequoiaproject.org) and other eHealth Exchange Participants who's Message Content may have been Breached to such information. CCHIE will also alert the PA eHealth Partnership Authority's ("Authority") Privacy Officer and other CCHIE Participants likely impacted through a secure email or phone call.

B. As soon as reasonably practicable, but no later than twenty-four (24) hours after determining that a Breach occurred, CCHIE shall provide notification to all Participants, including the eHealth Exchange and P3N, likely impacted by the Breach and the Coordinating Committee of such Breach. The notification should include sufficient information for the Coordinating Committee and the Authority to understand the nature of the Breach. For instance, such notification could include, to the extent available at the time of the notification, the following information:

1. Description of the Breach

2. Description of the roles of the people involved in the Breach (e.g. employees, users, service providers, unauthorized persons, etc.)
3. The type of health data Breached

4. CCHIE Participants likely impacted by Breach

5. Number of individuals or records impacted/estimated to be impacted by the Breach

6. Actions taken by the Participant to mitigate the Breach

7. Corrective action taken and steps planned to be taken to prevent a similar Breach

C. CCHIE shall supplement the information contained in the Breach notification as it becomes available and cooperate with other eHealth Exchange Participants, the Coordinating Committee, and the Authority in performing such actions as are required and as are necessary to mitigate the harmful effect of the Breach.

1. CCHIE shall not include any PHI in the notifications to the Coordinating Committee and the Authority.

VII. Revision History

DATE	AUTHOR	COMMENTS
12/05/2014	Jacqueline Smith	Creation of the policy
09/08/2015	Erika Jones	Updated template, changed language to include communication of breach to CCHIE Participants
9/14/2016	Jones/Szymanski	Changed contact info for Sequoia Project
10/10/2016	Szymanski	Changed “provide 1 to 2 sentence description” to just Description
05/13/2021	Keith Dukes	Updated formatting, corrected minor grammatical errors and verbiage – No major revisions applied