eHealth Exchange

Operating Policy & Procedure

SUBJECT: BREACH NOTIFICATION		
STATUS: FINAL – Approved by CC	POLICY #: OPP-7	
Effective Date: 2/16/2013	Version: 2.0	Page 1 of 5

I. Purpose

The privacy, security, and integrity of Message Content exchanged are essential. To help maintain the privacy, security and integrity of Message Content and promote trust among Participants, each Participant has agreed to notify certain other Participants and the Coordinating Committee of a Breach. This Policy sets forth the procedure by which a Participant and the Coordinating Committee will fulfill their respective Breach notification obligations under the Data Use Reciprocal and Support Agreement ("DURSA").

II. Policy

Breaches, as defined in the DURSA, are very serious events with potential for serious impact on Participants and the individuals whose Protected Health Information (PHI) is transmitted in Messages via the Exchange. A breach of PHI shall be treated as "discovered" as of the first day on which such breach is known to the organization, or, by exercising reasonable diligence would have been known to the organization (i.e. breaches by the organization's business associates). Thus, each Participant has the obligation to identify, notify, investigate and mitigate any known Breach or potential Breach, and when detection of a potential Breach has occurred, the Participant will notify the Coordinating Committee and any affected Participants of the potential Breach in accordance with the procedures herein.

The Coordinating Committee or its Designee Healtheway, Inc. (d/b/a/ "The Sequoia Project" and its "eHealth Exchange support staff") will conduct periodic reviews to evaluate and identified improvements to the Breach Notification process.

III. Procedure

A. Breach Notification Contact List

1. Participants shall provide eHealth Exchange support staff appropriate points of contact for Breach Notification and shall promptly notify the eHealth Exchange support staff if those points of contact change.
2. eHealth Exchange support staff shall maintain a list of Coordinating Committee Members as well as Participant contacts for Breach Notification purposes.
3. Participants are accountable for assuring there are mechanisms within their respective organizations to notify appropriate individuals regarding Breaches relative to the eHealth Exchange.

B. One-Hour Breach Alert

1. Within one (1) hour of discovering information that leads the Participant to reasonably believe that a Breach **may have occurred or could occur**, the Participant will:

    a. Immediately notify the Coordinating Committee of the potential Breach by sending an email to a dedicated e-mail address (hereinafter "Alert Email").

        i. The Alert Email is primarily intended to alert that a Breach may have occurred. Participants should use caution before relaying details of the potential Breach via e-mail.

    b. Immediately notify other Participants, who, in the judgment of the Participant making the alert, may have had a Breach of Message Content or otherwise are likely affected by the Breach.

2. Communication of Breach Notification

    a. Breach Notifications shall include a brief description of the information that lead the Participant to reasonably believe that a Breach may have occurred, a list of other Participants whose Message Content may have been Breached or otherwise are likely affected by the Breach, and a timeline for making a definitive determination on whether a Breach actually occurred.

    b. Participants are strongly urged to send Breach Notifications through a secure means, where appropriate and possible (e.g. fax, secure e-mail, posted on the Secure Site) and labeled as Confidential Participant Information.

3. If, on the basis of the information that the Participant has, the Participant believes that it should temporarily cease exchanging Message Content with all other Participants, it may undergo a service level interruption or voluntary suspension in accordance with Operating Policy and Procedure ("OPP") 3 (Participation – Changes, Suspension, and Termination).

C. Twenty-Four Hour Notification of Breach Determination

1. As soon as reasonably practicable, but no later than twenty-four (24) hours after determining whether **a Breach has occurred**, the Participant will:

    a. Immediately notify the Coordinating Committee whether the Breach occurred by sending an email to the Alert E-mail address or posting a Breach report to a Secure Site. .

    b. Send a notification of determination as to whether the Breach occurred to other Participants who are likely impacted by the Breach. Notifications sent to other Participants should be sent to the Breach Notification contact list.

2. Participants are strongly urged to send Breach Notifications through a secure means, where

appropriate and possible (e.g. fax, secure e-mail, posted on the Secure Site) and labeled as Confidential Participant Information. If the Breach was determined to have occurred, the notification should include sufficient information for the Coordinating Committee and other likely impacted 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:

- One or two sentence description of the Breach
- Description of the roles of the people involved in the Breach (e.g. employees, Participant Users, service providers, unauthorized persons, etc.)
- The type of Message Content Breached
- Participants likely impacted by Breach
- Number of individuals or records impacted/estimated to be impacted by the Breach
- Actions taken by the Participant to mitigate the Breach
- Current Status of the Breach (under investigation or resolved)
- Corrective action taken and steps planned to be taken to prevent a similar Breach.

The notification shall not include any Protected Health Information (PHI). Participants are strongly urged to label the notification (e.g. subject line or posting, etc.) as Confidential Participant Information.

3. The Participant shall have a duty to supplement the information contained in the notification as it becomes available. Supplemental information should be uploaded to the Secure Site and directed to the same addresses used for the original notification. Participants are strongly urged to label (e.g. subject line or posting, etc.) the supplemental information as Confidential Participant Information.
4. If, on the basis of the information that the Participant has, the Participant believes that it should temporarily cease exchanging Message Content with all other Participants through the eHealth Exchange, it may undergo a service level interruption or voluntary suspension in accordance with Operating Policy and Procedure 3 (Participation – Changes, Suspension, and Termination).

D. Coordinating Committee Disposition of Breach Alerts and Notifications

1. At the earliest possible time, the Coordinating Committee Chair shall schedule a meeting of the Committee upon receipt of the Breach alert and notification for the purpose of reviewing the notification and determining the following:
    a. The impact of the Breach or potential Breach on the privacy, security and integrity of Message Content exchanged through the eHealth Exchange;

b. Whether the Coordinating Committee needs to take any action to suspend the Participant(s) involved in the Breach or potential Breach in accordance with the DURSA and the Change, Suspension and Termination Policy;

c. Whether other Participants that have not been notified of the Breach or potential Breach would benefit from a summary of the notification or alert; or whether a summary of the notification or alert to the other Participants would enhance the security of the eHealth Exchange; and,

   i. If the Coordinating Committee determines that a summary should be distributed to Participants, the Coordinating Committee will distribute such summary in a timely manner.

   ii. This summary shall not identify any of the Participants or individuals involved in the Breach.

d. Whether the Coordinating Committee should take any other measures in response to the notification or alert.

2. If a Participant reports a potential Breach and later determines that a Breach did not, in fact, occur, the Coordinating Committee has final discretion regarding whether a meeting is necessary to discuss disposition of the event.

3. The Coordinating Committee is permitted to request additional information from the Participant(s) involved in the Breach or potential Breach to fulfill its responsibilities. However, with respect to potential Breach alerts, the Coordinating Committee is encouraged to hold inquiries and requests for additional information to allow the Participant time to determine whether a Breach actually occurred.

4. If, on the basis of the Breach alert or notification, a Participant desires to cease exchanging Message Content with Participant(s) involved in the potential or actual Breach, pursuant to the DURSA, such Participant must notify eHealth Exchange support staff of such cessation. eHealth Exchange support staff will notify Members of the Coordinating Committee of each cessation notification and keep a log of all such cessations for the Coordinating Committee's review.

5. If it is determined a Breach occurred, once sufficient information about the Breach becomes available, the Coordinating Committee will meet at the earliest possible time to determine whether the actions taken by the Participant(s) involved in the Breach are adequate to mitigate the Breach and prevent a similar Breach from occurring in the future. Once the Coordinating Committee is satisfied that the Participant(s) have taken all appropriate measures, the Coordinating Committee will deem the Breach resolved. Participants will update and inform the Coordinating Committee as soon as possible regarding new information involving the Breach.

   a. This resolution will be communicated to all Participant(s) involved in the Breach and those Participants that ceased exchanging Message Content with the Participant(s) involved in the Breach (if applicable).

b. If a Participant does not resume the exchange of Message Content with the Participant(s) involved in the Breach, such Participant(s) involved in the Breach and cessation are encouraged to engage in the Dispute Resolution Process pursuant to the DURSA.

IV. Definitions

Pursuant to Section 1(c) of the DURSA, "Breach" shall mean the unauthorized acquisition, access, disclosure, or use of Message Content through the eHealth Exchange. The term ''Breach'' does not include the following:

(i) Any unintentional acquisition, access, disclosure, or use of Message Content through the eHealth Exchange by an employee or individual acting under the authority of a Participant or Participant User if—

(I) Such acquisition, access, disclosure, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with the Participant or Participant User; and

(II) Such Message Content is not further acquired, accessed, used, or disclosed by such employee or individual; or

(ii) Any acquisition, access, use or disclosure of information contained in or available through the Participant's System where such acquisition, access, use or disclosure was not directly related to transmission of Message Content through the NHIN.

DURSA: Data Use and Reciprocal Support Agreement

Secure Site: A secure web portal where information for eHealth Exchange Participants and Coordinating Committee members will be maintained pursuant to OPP 6 (Information Handling).

All other capitalized terms, if not defined herein, shall have the same meaning as set forth in the DURSA or the Coordinating Committee Operating Policies and Procedures.

V. References

- DURSA
- 14.03 – Breach Notification
- 16 – Confidential Participant Information
- 19 – Term, Suspension and Termination
- 21 – Dispute Resolution

VI. Related Policies and Procedures

- OPP #3 - Changes, Suspension and Termination; Information Handling

VII. Version History

	Date	Author	Comment
1	11/29/09	Erin Whaley and Steve Gravely	Original.
2	12/4/09	Erin Whaley and Steve Gravely	Revised to incorporate comments from 12/1/09 OP&P Team call.
3	12/23/09	Erin Whaley and Steve Gravely	Revised to incorporate comments from 12/8/09 OP&P Team call and cross reference to OP&P 3 for service level interruptions and voluntary suspensions.
4	1/22/10	Erin Whaley and Steve Gravely	Revised to incorporate minor stylistic changes as approved by Coordinating Committee during 1/21/10 call
5	3/27/12	Marcia Gonzales, Edye Taylor and Mariann Yeager	Revised to reflect amended DURSA
6	4/17/12 1/14/13	OPP Task Group Mariann Yeager Christina Arenas	Revised following OPP Task Group meeting on 4/17/12. Revised to incorporate post-transition responsibilities.
7	1/23/13	Christina Arenas	Deleted remaining occurrences of NHIN in the definitions section
8	8/15/16	Theresa Wiebold	Administrative updates to remove references to Healtheway