eHealth Exchange

Operating Policy and Procedure

Subject: Adverse Security Event Notification		
Status: FINAL – Approved by CC	POLICY #: OPP-7	
Effective Date: 8/1/2020	Version: 3.0	Page 1 of 7

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 an Adverse Security Event. This Policy sets forth the procedure by which a Participant and the Coordinating Committee will fulfill their respective Adverse Security Event notification obligations under the Data Use Reciprocal and Support Agreement ("DURSA").

II. *Policy*

Adverse Security Events, 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. An Adverse Security Event shall be treated as "discovered" as of the first day on which such Adverse Security Event is known to the organization, or, by exercising reasonable diligence would have been known to the organization (i.e. Adverse Security Events suffered by the organization's business associates). Thus, each Participant has the obligation to identify, notify, investigate and mitigate any known Adverse Security Event When detection of an Adverse Security Event has occurred, the Participant will notify the Coordinating Committee and any affected Participants of the Adverse Security Event in accordance with the procedures herein.

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

III. *Procedure*

A. Adverse Security Event Notification Contact List

1. Participants shall provide eHealth Exchange support staff appropriate points of contact for Adverse Security Event 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 Adverse Security Event Notification purposes.
3. Participants are accountable for assuring there are mechanisms within their respective organizations to notify appropriate individuals regarding Adverse Security Events relative to the eHealth Exchange.

B. Adverse Security Events involving Federal Participants: One-Hour Adverse Security Event Alert

1. Within one (1) hour of discovering information that leads the Participant to reasonably believe that an adverse security event **may have occurred**, and that such event may involve a Federal Participant, the Participant shall:
    a. Immediately alert the Federal Participant in accordance with the procedures and contacts provided by such Federal Participant.
    b. Within twenty-four (24) hours after determining that an Adverse Security Event may have occurred and is likely to have an adverse impact on a Federal Participant(s), Participant shall provide notification to the Coordinating Committee of the potential Adverse Security Event by sending an email to the dedicated e-mail address: securityevent@ehealthexchange.org (hereinafter "Alert Email").
        i. The Alert Email is primarily intended to alert that an Adverse Security Event may have occurred. Participants should use caution before relaying details of the potential Adverse Security Event via e-mail.
    c. Within twenty-four (24) hours after determining that an Adverse Security Event has occurred and is likely to have an adverse impact on a Federal Participant(s), Participant shall provide a notification to all such Participants that may have had an Adverse Security Event of Message Content or otherwise are likely affected by the Adverse Security Event in accordance with the procedures and contacts provided by such Federal Participant.

2. Communication of Adverse Security Event Notification
    a. Adverse Security Event Notifications shall include a brief description of the information that lead the Participant to reasonably believe that an Adverse Security Event may have occurred, a list of other Participants whose Message Content may have been impacted or otherwise are likely affected by the Adverse Security Event, and a timeline for making a definitive determination on whether an Adverse Security Event actually occurred.
    b. Participants are strongly urged to send Adverse Security Event Notifications through a secure means, when appropriate 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. Adverse Security Events involving All Participants: Five Business Day Notification of Adverse Security Event Determination

1. As soon as reasonably practicable, but no later than five (5) business days after determining whether **an Adverse Security Event has occurred** and is likely to have an adverse impact on the Network or another Participant, the Participant will:

    a. Immediately notify the Coordinating Committee whether the Adverse Security Event occurred by sending an email to the Alert e-mail: securityevent@ehealthexchange.org.

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

2. Participants are to send Adverse Security Event Notifications through a secure means, when appropriate and labeled as Confidential Participant Information. If the Adverse Security Event 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 Adverse Security Event. 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 Adverse Security Event
    - Description of the roles of the people involved in the Adverse Security Event (e.g. employees, Participant Users, service providers, unauthorized persons, etc.)
    - The type of Message Content involved in the Adverse Security Event
    - Participants likely impacted by the Adverse Security Event
    - Number of individuals or records impacted/estimated to be impacted by the Adverse Security Event
    - Actions taken by the Participant to mitigate the Adverse Security Event
    - Current Status of the Adverse Security Event (under investigation or resolved)
    - Corrective action taken and steps planned to be taken to prevent a similar Adverse Security Event.

    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 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. <u>Coordinating Committee Disposition of Adverse Security Event Alerts and Notifications</u>

1. At the earliest possible time, the Coordinating Committee Chair shall schedule a meeting of the Committee upon receipt of the Adverse Security Event alert and notification for the purpose of reviewing the notification and determining the following:
    a. The impact of the Adverse Security Event or potential Adverse Security Event 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 Adverse Security Event or potential Adverse Security Event in accordance with the DURSA and the Change, Suspension and Termination Policy;
    c. Whether other Participants that have not been notified of the Adverse Security Event or potential Adverse Security Event 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 Adverse Security Event.
    d. Whether the Coordinating Committee should take any other measures in response to the notification or alert.
2. If a Participant reports a potential Adverse Security Event and later determines that an Adverse Security Event 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 Adverse Security Event or potential Adverse Security Event to fulfill its responsibilities. However, with respect to potential Adverse Security Event alerts, the Coordinating Committee is encouraged to hold inquiries and requests for additional information to allow the Participant time to determine whether an Adverse Security Event actually occurred.
4. If, on the basis of the Adverse Security Event alert or notification, a Participant desires to cease exchanging Message Content with Participant(s) involved in the potential or actual Adverse Security Event, 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 an Adverse Security Event occurred, once sufficient information about the Adverse Security Event 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 Adverse Security Event are adequate to mitigate the Adverse Security Event and prevent a similar Adverse Security Event 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 Adverse Security Event resolved. Participants will update and inform the Coordinating Committee as soon as possible regarding new information involving the Adverse Security Event.

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

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

IV. ***Definitions***

Adverse Security Event: shall mean the unauthorized acquisition, access, disclosure, or use of unencrypted Message Content while in the process of being transacted in a manner permitted by this Agreement by anyone who is not a Participant or Participant User or by a Participant or Participant User in any manner that is not a Permitted Purpose under this Agreement. For the avoidance of doubt, an "Adverse Security Event" under this Agreement does not include the following:

(i) any unintentional acquisition, access, disclosure, or use of Message Content 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 unencrypted Message Content is not further acquired, accessed, disclosed or used by such employee or individual; or

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

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 or the Coordinating Committee Operating Policies and Procedures.

V. *References*

"Restatement II of the Data Use and Reciprocal Support Agreement (DURSA)", Version Date: August 13, 2019

- Section 14.04, Adverse Security Event Notification
- Section 16, Confidential Participant Information
- Section 19, Term, Suspension and Termination
- Section 21, Dispute Resolution

VI. *Related Policies and Procedures*

- OPP #3, Changes, Suspension and Termination
- OPP #6, Information Handling
- OPP #9, Digital Credentials

VII. *Version History*

ID	Date	Author	Comments
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 OPP Team call.
3	12/23/09	Erin Whaley and Steve Gravely	Revised to incorporate comments from 12/8/09 OPP Team call and cross-reference to OPP 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	OPP Task Group, Mariann Yeager and 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
9	6/2020	Jay Nakashima	Updated language to reflect newest DURSA amendment changes; Updated formatting for consistency and readability