

Operating Policy ~~& and~~ Procedure

SUBJECT Subject: BREACH Adverse Security Event NotificationNOTIFICATION		
STATUS Status: FINAL – Approved by CC	POLICY #: OPP-7	
Effective Date: 2/16/2013	Version: 2.0	Page 1 of 8Page 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 an Adverse Security Event Breach. This Policy sets forth the procedure by which a Participant and the Coordinating Committee will fulfill their respective Breach Adverse Security Event notification obligations under the Data Use Reciprocal and Support Agreement (“DURSA”).

II. Policy

~~Breaches~~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 breach of PHI shall be treated as “discovered” as of the first day on which such ~~breach~~ Adverse Security Event is known to the organization, or, by exercising reasonable diligence would have been known to the organization (i.e. ~~breaches~~ 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 EventBreach or ~~potential Adverse Security EventBreach~~, and ~~—w~~When detection of an potential Adverse Security EventBreach has occurred, the Participant will notify the Coordinating Committee and any affected Participants of the ~~potential~~ Adverse Security EventBreach in accordance with the procedures herein.

The Coordinating Committee or its Designee Healthway, Inc. (d/b/a/ “The ~~eE~~Health Exchange” and its “eHealth Exchange support staff”) will conduct periodic reviews to evaluate and identified improvements to the Adverse Security EventBreach Notification process.

III. Procedure

A. BreachAdverse Security Event Notification Contact List

1. Participants shall provide eHealth Exchange support staff appropriate points of contact for BreachAdverse 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 BreachAdverse Security Event Notification purposes.

Operating Policy ~~& and~~ Procedure

SUBJECT Subject: BREACH Adverse Security Event Notification NOTIFICATION		
STATUS Status: FINAL – Approved by CC	POLICY #: OPP-7	
Effective Date: 2/16/2013	Version: 2.0	Page 2 of 8 Page 1 of 5

3. Participants are accountable for assuring there are mechanisms within their respective organizations to notify appropriate individuals regarding Adverse Security Event~~Breaches~~ relative to the eHealth Exchange.

B. One-Hour Breach~~Adverse Security Event~~ Alert

1. Within one (1) hour of discovering information that leads the Participant to reasonably believe that an adverse security event ~~Breach~~ **may have occurred or could occur, and that such event may involve a Federal Participant,** the Participant ~~will~~shall:
 - a. Immediately alert the Federal Participant in accordance with the procedures and contacts provided by such Federal Participant.
 - ~~a.b.~~ Immediately ~~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 notify~~ the Coordinating Committee of the potential Breach~~Adverse Security Event~~ by sending an email to ~~a the~~ dedicated e-mail address: securityevent@ehealthexchange.org (hereinafter “Alert Email”).
 - i. ~~i.~~ The Alert Email is primarily intended to alert that an Breach~~Adverse Security Event~~ may have occurred. Participants should use caution before relaying details of the potential Breach~~Adverse Security Event~~ via e-mail.
 - ~~b.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. Immediately notify other Participants, who, in the judgment of the Participant making the alert, may have had an Breach~~Adverse Security Event~~ of Message Content or otherwise are likely affected by the Breach~~Adverse Security Event~~.
2. Communication of Breach~~Adverse Security Event~~ Notification
 - a. Breach~~Adverse Security Event~~ Notifications shall include a brief description of the information that lead the Participant to reasonably believe that an Breach~~Adverse~~

Operating Policy ~~&~~ and Procedure

SUBJECT <u>Subject</u> : BREACH <u>Adverse Security Event Notification</u> NOTIFICATION		
STATUS <u>Status</u> : FINAL – Approved by CC	POLICY # : OPP-7	
Effective Date : <u>2/16/2013</u>	Version : <u>2.0</u>	Page <u>3 of 8</u> Page 1 of 5

Security Event may have occurred, a list of other Participants whose Message Content may have been ~~Breached~~ impacted or otherwise are likely affected by the ~~Breach~~ Adverse Security Event, and a timeline for making a definitive determination on whether an ~~Breach~~ Adverse Security Event actually occurred.

- b. Participants are strongly urged to send Breach Adverse Security Event Notifications through a secure means, ~~where~~ when 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~~ Five Business Day Notification of ~~Breach~~ Adverse Security Event Determination

1. As soon as reasonably practicable, but no later than ~~twenty-four~~ five (24~~5~~) ~~hours~~ 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 ~~Breach~~ occurred by sending an email to the Alert ~~E~~ e-mail: securityevent@ehealthexchange.org ~~address or posting a Breach report to a Secure Site.~~
 - ~~e.a.~~ Send a notification of determination as to whether the Adverse Security Event ~~Breach~~ occurred to other Participants who are likely impacted by the Adverse Security Event ~~Breach~~. Notifications sent to other Participants should be sent to the Adverse Security Event ~~Breach~~ Notification contact list.
2. Participants are ~~strongly urged~~ to send Adverse Security Event ~~Breach~~ Notifications through a secure means, ~~where~~ when appropriate ~~and possible (e.g. fax, secure e-mail, posted on the Secure Site)~~ and labeled as Confidential Participant Information. If the Adverse Security Event ~~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 Adverse Security Event ~~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 Adverse Security Event ~~Breach~~
 - Description of the roles of the people involved in the Adverse Security Event ~~Breach~~ (e.g. employees, Participant Users, service providers, unauthorized persons, etc.)

Operating Policy & Procedure

SUBJECT Subject: <u>BREACH Adverse Security Event Notification</u> NOTIFICATION		
STATUS Status: FINAL – Approved by CC	POLICY #: OPP-7	
Effective Date: <u>2/16/2013</u>	Version: <u>2.0</u>	Page <u>4 of 8</u> Page 1 of 5

- The type of Message Content ~~Breached~~impacted involved in the Adverse Security Event
- Participants likely impacted by the Adverse Security Event~~Breach~~
- Number of individuals or records impacted/estimated to be impacted by the Adverse Security Event~~Breach~~
- Actions taken by the Participant to mitigate the Adverse Security Event~~Breach~~
- Current Status of the Adverse Security Event~~Breach~~ (under investigation or resolved)
- Corrective action taken and steps planned to be taken to prevent a similar Adverse Security Event~~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~~Adverse Security Event Alerts and Notifications

1. At the earliest possible time, the Coordinating Committee Chair shall schedule a meeting of the Committee upon receipt of the BreachAdverse Security Event alert and notification for the purpose of reviewing the notification and determining the following:
 - a. The impact of the BreachAdverse Security Event or potential BreachAdverse 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 BreachAdverse Security Event or potential BreachAdverse 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 BreachAdverse Security Event or potential BreachAdverse Security Event would benefit from a summary of the

Operating Policy ~~&and~~ Procedure

SUBJECT Subject: <u>BREACH Adverse Security Event Notification</u> NOTIFICATION		
STATUS Status: FINAL – Approved by CC	POLICY #: OPP-7	
Effective Date: 2/16/2013	Version: 2.0	Page 5 of 8 Page 1 of 5

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.~~ 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.~~ ii. This summary shall not identify any of the Participants or individuals involved in the Breach 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 Breach Adverse Security Event and later determines that an Breach 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 Breach Adverse Security Event or potential Breach Adverse Security Event to fulfill its responsibilities. However, with respect to potential Breach 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 Breach Adverse Security Event actually occurred.
4. If, on the basis of the Breach Adverse Security Event alert or notification, a Participant desires to cease exchanging Message Content with Participant(s) involved in the potential or actual Breach 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 Breach Adverse Security Event occurred, once sufficient information about the Breach 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 Breach Adverse Security Event are adequate to mitigate the Breach Adverse Security Event and prevent a similar Breach 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 Breach Adverse Security Event resolved. Participants will update and inform the Coordinating Committee as soon as possible regarding new information involving the Breach Adverse Security Event.

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

a.

Operating Policy ~~& and~~ Procedure

SUBJECT Subject: <u>BREACH Adverse Security Event Notification</u> NOTIFICATION		
STATUS Status: FINAL – Approved by CC	POLICY #: OPP-7	
Effective Date: <u>2/16/2013</u>	Version: <u>2.0</u>	<u>Page 6 of 8</u> Page 1 of 5

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

IV. Definitions

Pursuant to Section 1(~~ed~~) of the DURSA, “Breach Adverse Security Event” shall mean the unauthorized acquisition, access, disclosure, or use of unencrypted Message Content, ~~through the eHealth Exchange~~. The term “Breach Adverse Security Event” 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 unencrypted 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

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

- Section 14.043—Breach Adverse Security Event Notification
- Section 16—Confidential Participant Information
- Section 19—Term, Suspension and Termination
- Section 21—Dispute Resolution

Operating Policy ~~&~~ and Procedure

SUBJECT Subject: <u>BREACH-Adverse Security Event Notification</u> NOTIFICATION		
STATUS Status: FINAL – Approved by CC	POLICY #: OPP-7	
Effective Date: 2/16/2013	Version: 2.0	Page 7 of 8 Page 1 of 5

VI. Related Policies and Procedures

- OPP #3–Changes, Suspension and Termination;
- OPP #6, Information Handling

VII. Version History

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

Operating Policy ~~&~~ and Procedure

SUBJECT <u>Subject:</u> BREACH Adverse Security Event Notification NOTIFICATION		
STATUS <u>Status:</u> FINAL – Approved by CC	POLICY #: OPP-7	
Effective Date: 2/16/2013	Version: 2.0	Page 8 of 8 Page 1 of 5

9	2/2020	Jay Nakashima	<u>Updated language to reflect newest DURSA amendment changes; Updated formatting for consistency and readability</u>
---	--------	---------------	---

Date Author Comment

-
- 1 ~~11/29/09 Erin Whaley and Original. Steve Gravely~~
 - 2 ~~12/4/09 Erin Whaley and Revised to incorporate comments from 12/1/09 OP&P Team call. Steve Gravely~~
 - 3 ~~12/23/09 Erin Whaley and Revised to incorporate comments from 12/8/09 OP&P Team call Steve Gravely and cross reference to OP&P 3 for service level interruptions and voluntary suspensions.~~
 - 4 ~~1/22/10 Erin Whaley and Revised to incorporate minor stylistic changes as approved by Steve Gravely Coordinating Committee during 1/21/10 call~~
 - 5 ~~3/27/12 Marcia Gonzales, Revised to reflect amended DURSA Edye Taylor and Mariann Yeager~~
 - 6 ~~4/17/12 OPP Task Group Revised following OPP Task Group meeting on 4/17/12. 1/14/13 Mariann Yeager Revised to incorporate post-transition responsibilities. Christina Arenas~~
 - 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 Healthway~~