	Privacy	Rio Grande Valley HIE	Policy: P11
	Effective Date 11/06/2015	**Last Date Revised/Updated** 11/06/2015	**Date Board Approved:** 11/06/2015
Subject: **Breach Notification and Mitigation**			

FEDERAL REGULATION:

45 CFR §§ 164.400-414
TX Business & Commerce Code 521.053

POLICY:

1. PURPOSE

The purpose of this Breach Notification Policy is to provide guidance to the staff of Rio Grande Valley Health Information Exchange when there is a breach an acquisition, access, use, or disclosure of the unsecured protected health information in a manner not permitted under the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and its implementing rules and regulations, which compromises the security or privacy of the Protected Health Information (PHI). HIPAA requires that RGV HIE notify individuals whose unsecured PHI has been compromised by such a breach. In certain circumstances, RGV HIE must also report such breaches to the Secretary of HHS and through the media. RGV HIE's breach notification process will be carried out in compliance with the Health Information Technology for Economic and Clinical Health (HITECH) Act of the American Recovery and Reinvestment Act of 2009 and its implementing rules and regulations, each as may be amended from time to time, including those regulatory amendments of the Department of Health and Human Services published at 78 Fed. Reg. 5566 (Jan. 25, 2013), collectively "HIPAA."

2. DEFINITIONS

2.1 **Breach**. Breach means the acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted under HIPAA, which compromises the security or privacy of the protected health information. Breach excludes:

2.1.1 Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or business associate if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under HIPAA.

2.1.2 Any inadvertent disclosure by a person who is authorized to access protection health information at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which

the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under HIPAA.

2.1.3 A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

2.2 **DURSA Breach:** Breach in this context is: "the unauthorized acquisition, access, disclosure, or use of Message Content while Transacting such Message Content"

•A breach does not include either of the following:

1. 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:
   • Made in good faith and within the course / scope of that individual's employment / engagement; and
   • The information is not further acquired, accessed, disclosed or used by the individual;
2. Any acquisition, access, disclosure or use of information contained in or available through the Participant's System that was not directly related to Transacting Message Content.
   • The breach reporting process is NOT intended to address any obligations for notifying consumers of breaches, but simply establishes an obligation for Participants to notify each other and the Coordinating Committee when Breaches occur to facilitate an appropriate response.

2.3 **Protected Health Information (PHI)**. Protected health information means individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.

2.4 **Transact.** Transact means to send, request, receive, assert, respond to, submit, route, subscribe to, or publish Message Content containing PHI during the course of HIE operations, testing or reporting.

2.5 **Unsecured Protected Health Information (Unsecured PHI)**. Unsecured PHI means any PHI which is not unusable, unreadable, or indecipherable to unauthorized persons through the use of technology or methodology, such as encryption or destruction, as specified by the HSS Secretary.

2.6 **Workforce**. Workforce means employees, volunteers, trainees, and other persons under the direct control of HASA, whether or not they are paid by RGV HIE.

3. POLICY AND PROCEDURES

In summary, HIPAA requires that covered entities notify individuals whose unsecured protected health information has been impermissibly accessed, acquired, used, or disclosed, compromising the security or privacy of the protected health information. The notification requirements only apply to breaches of unsecured PHI. In other words, if PHI is encrypted or destroyed in accordance with the HIPAA guidance, there is a "safe harbor" and notification is not required.

3.1 **Discovery of Breach**. A breach shall be treated as discovered as of the first day on which such breach is known to RGV HIE or, by exercising reasonable diligence, would have been known to RGV HIE or any person, other than the person committing the breach, who is a workforce member or agent of RGV HIE.

Workforce members who believe that patient information has been used or disclosed in any way that compromises the security or privacy of that information shall immediately notify the RGV HIE privacy officer.

Following the discovery of a potential breach, RGV HIE shall begin an investigation, and conduct a risk assessment. In accordance with the Texas SLTA and the federal DURSA, RGV HIE will alert other participants whose message content may have been breached and the appropriate coordinating committee – HIE Texas or Healtheway - to such information of the potential breach within one (1) hour of learning of the potential breach should it be deemed to qualify as a DURSA Breach.

As soon as reasonably practicable, but no later than twenty-four (24) hours after determining that a Breach has occurred, RGV HIE shall provide a notification to all HIE Texas and Healtheway participants likely impacted by the DURSA Breach and the Coordinating Committee of such DURSA Breach. The notification will include sufficient information for the Coordinating Committee to understand the nature of the breach. Notification to these entities by RGV HIE will 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 the 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.

Based on the results of the risk assessment, RGV HIE will begin the process of notifying each individual whose PHI has been, or is reasonably believed by RGV HIE to have been, accessed, acquired, used, or disclosed as a result of the breach. This process will include contacting any covered entity to whom RGV HIE is a business associate whose data might have been breached. RGV HIE shall also begin the process of determining what notifications are required or should be made, if any, to the Secretary of the Department of Health and Human Services (HHS) and media outlets.

3.2 **Breach Investigation**. RGV HIE shall name an individual to act as the investigator of the breach. The investigator shall be responsible for the management of the breach investigation, completion of the risk assessment, and coordinating with vendors and contributing members as appropriate. RGV HIE's entire workforce is expected to assist management in this investigation as requested. The investigator shall be the key facilitator for all breach notification processes.

3.3 **Risk Assessment**. For breach response and notification purposes, a breach is presumed to have occurred unless RGV HIE can demonstrate that there is a low probability that the PHI has been compromised based on, at minimum, the following risk factors:

3.3.1 The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.

3.3.2 The unauthorized person who used the PHI or to whom the disclosure was made.

3.3.2.1 Does the unauthorized person have obligations to protect the PHI's privacy and security?

3.3.2.2 Does the unauthorized person have the ability to re-identify the PHI?

3.3.3 Whether the PHI was actually acquired or viewed.

3.3.3.1 Does analysis of a stolen and recovered device show that PHI stored on the device was never accessed?

3.3.4 The extent to which the risk to the PHI has been mitigated.

3.3.4.1 Can RGV HIE obtain the unauthorized person's satisfactory assurances that the PHI will not be further used or disclosed or will be destroyed?

The evaluation should consider these factors, or more, in combination to determine the overall probability that PHI has been compromised. The risk assessment should be thorough and completed in good faith, and the conclusions should be reasonable.

Based on the outcome of the risk assessment, RGV HIE will determine the need to move forward with breach notification. The investigator must document the risk assessment and the outcome of the risk assessment process. All documentation related to the breach investigation, including the risk assessment must be retained for a minimum of six years.

3.4 **Notification: Individuals Affected**. If it is determined that breach notification must be sent to affected individuals, RGV HIE will use a standard breach notification letter (as modified for the specific breach), and it will be sent out to all affected individuals as well as covered entities to which RGV HIE is a business associate. RGV HIE also has the discretion to provide notification following an impermissible use or disclosure of PHI without performing a risk assessment, if RGV HIE so chooses. Notice to affected individuals shall be written in plain language and must contain the following information, which elements shall be included in RGV HIE's standard breach notification letter:

3.4.1 A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.

3.4.2 A description of the types of unsecured protected health information that was involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved).

3.4.3 Any steps the individuals should take to protect themselves from potential harm resulting from the breach.

3.4.4 A brief description of what RGV HIE is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.

3.4.5 Contact procedures for individuals to ask questions or learn additional information, which includes a telephone number, email address, website, or postal address.

This letter will be sent by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification shall be provided in one or more mailings, as information is available. If RGV HIE knows that the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first-class mail to the next of kin or person representative shall be carried out.

If there is insufficient or out-of-date contact information that precludes direct written or electronic notification, a substitute form of notice reasonably calculated to reach the individual shall be provided.

If there is insufficient or out-of-date contact information for fewer than 10 individuals, then the substitute notice may be provided by an alternative form of written notice, by telephone, or by other means. If there is insufficient or out-of-date contact information for 10 or more individuals, then the substitute notice shall be in the form of either a conspicuous posting for a period of 90 days on the home page of RGV HIE's website, or a conspicuous notice in major print or broadcast media in RGV HIE's geographic areas where the individuals affected by the breach likely reside. The notice shall include a toll-free number that remains active for at least 90 days where an individual can learn whether his or her PHI may be included in the breach.

Notice to affected individuals shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach. If RGV HIE determines that notification requires urgency because of possible imminent misuse of unsecured PHI, notification may be provided by telephone or other means, as appropriate, in addition to the methods noted above. As per HIPAA guidelines, it is the responsibility of RGV HIE to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of any delay.

3.5 **Notification: HHS**. In the event a breach of unsecured PHI affects 500 or more of RGV HIE's individual records, HHS will be notified at the same time notice is made to the affected individuals, in the matter specified on the HHS website. If fewer than 500 of RGV HIE's encounter records are affected, RGV HIE will maintain a log of the breaches to be submitted annually to the Secretary of HHS no later than 60 days after the end of each calendar year, in the manner specific on the HHS website. The submission shall include all breaches discovered during the preceding calendar year.

3.6 **Notification: Media**. In the event the breach affects more than 500 residents of a state, prominent media outlets serving the state and regional area will be notified without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach. The notice shall be provided in the form of a press release.
If a person is required by this section to notify at one time more than 10,000 persons of a breach of system security, the person shall also notify each consumer reporting agency, as defined by 15 U.S.C. Section 1681a, that maintains files on consumers on a nationwide basis, of the timing, distribution, and content of the notices. The person shall provide the notice required by this subsection without unreasonable delay.

3.7 **Delay of Notification Authorized for Law Enforcement Purposes**. If a law enforcement official states to the Practice or a business associate that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, RGV HIE shall:

3.7.1 If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or
3.7.2 If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during that time.

This applies to notices made to individuals, the media, HHS, and by business associates.

3.8 **Maintenance of Breach Information**. RGV HIE shall maintain a process to record or log all breaches of unsecured PHI, regardless of the number of patients affected. The following information should be collected for each breach:

3.8.1 A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of patients affected, if known.
3.8.2 A description of the types of unsecured protected health information that was involved in the breach (such as full name, social security number, date of birth, home address, account number, other).
3.8.3 A description of the action taken with regard to notification of patients regarding the breach.
3.8.4 Steps taken to mitigate the breach and prevent future occurrences.

3.9 **Business Associate Responsibilities**. RGV HIEs business associates shall, in accordance to their respective Business Associate agreements, notify RGV of any such breach. Business Associate will, following the discovery of a HIPAA Breach, notify RGV HIE without unreasonable delay and in no event later than the earlier of the maximum of time allowable under applicable law or three (3) business days after Business Associate discovers such HIPAA Breach, unless Business Associate is prevented from doing so by 45 C.F.R. §164.412 concerning law enforcement investigations.

The business associate shall provide RGV HIE with any other available information that RGV HIE is required to include in notification to the individual at the time of the notification or promptly thereafter as information becomes available. Upon notification by the business associate of discovery of a breach, RGV HIE will be responsible for notifying affected individuals, unless otherwise agreed upon by the business associate to notify the affected individuals.

3.10 **Workforce Training**. RGV HIE shall train all members of its workforce on the policies and procedures with respect to PHI as necessary and appropriate for the members to carry out their job responsibilities. Workforce members shall also be trained as to how to identify and report breaches within the Practice. RGV HIE trains its employees annually on the policies and procedures with respect to PHI.

3.11 **Complaints**. RGV HIE provides a process for individuals to make complaints concerning HASA privacy policies and procedures or its compliance with such policies and procedures. Individuals also have the right to complain about RGV HIE's breach notification processes. These complaint procedures are outlined in the RGV HIE notice of privacy practices.

3.12 **Sanctions**. Members of the RGV HIE workforce who fail to comply with this policy shall be subject to disciplinary action, up to and including termination.

3.13 **Retaliation/Waiver**. RGV HIE may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for exercising his or her privacy rights. Individuals shall not be required to waive their privacy rights as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

3.14 **Burden of Proof**. As per HIPAA, RGV HIE has the burden of proof for demonstrating that all notifications were made as required or that the use or disclosure did not constitute a breach.

REVIEWED:
REVISED:

APPROVAL: _____

Effective Date:

By:

Title:

SUPERCEDES: _____
Policy Title and Number

REVIEW:

_____ _____ _____
Date **Date** **Date**