	Security	Rio Grande Valley HIE	Policy: S9
	Effective Date 11/20/2015	**Last Date Revised/Updated** 11/20/2015	**Date Board Approved:** 11/20/2015
Subject: **Administrative Safeguard – Contingency Planning**			

FEDERAL REGULATION:

45 CFR 164.308(a)(7)

POLICY:

The Rio Grande Valley Health Information Exchange (RGV HIE) has adopted this policy to ensure that its response to an emergency or other occurrence that damages systems that contain ePHI complies with the Security Regulations. This Policy covers the procedures that RGV HIE has developed for implementation in the event of an emergency or other occurrence, such as fire, vandalism, system failure, and natural disaster, when any system that contains ePHI is affected, including:

- **Disaster Recovery Plan 164.308(a)(7)(ii)(B) –** Procedures to restore any loss of data
- **Data Backup Plan 164.308(a)(7)(ii)(A) –** Procedures to create and maintain retrievable exact copies of ePHI
- **Emergency Mode Operation Plan 164.308(a)(7)(ii)(C)** – Procedures to enable continuation of critical business processes for the protection of the security of ePHI while operating in an emergency mode
- **Testing and Revision Procedures 164.308(a)(7)(ii)(D) –** Procedures for periodic testing and revision of contingency plans
- **Key Functions Criticality Analysis 164.308(a)(7)(ii)(E)** – Assessment of the relative criticality of specific applications and data in support of contingency plan components

RGV HIE assets are infrastructure that contains, maintains, or transmits ePHI. To develop a contingency plan, HIE shall identify and inventory HIE assets including applications and/or mobile devices. RGV HIE will also obtain an inventory of assets subject to contingency planning from RGV HIE technology vendors.

PROCEDURE:

Disaster Recovery Plan

RGV HIE does not store ePHI in its offices, including any laptops or other devices. Rather, all ePHI is stored on systems managed by RGV HIE's technology vendors. RGV HIE shall require its technology vendors to develop a Disaster Recovery Plan, in compliance with HIPAA, as follows:

- A Disaster Recovery Plan shall be established to recover from the loss of data due to an emergency or disaster such as fire, vandalism, terrorism, system failure, or natural disaster effecting systems containing ePHI.
- The Disaster Recovery Plan shall include processes to restore or recover any loss of ePHI and the systems needed to make that ePHI available in a timely manner.
- The Disaster Recovery Plan shall include procedures to restore ePHI from data backups in the case of a disaster causing data loss.
- The Disaster Recovery Plan shall include procedures to log system outages, failures, and data loss to critical systems, and procedures to train the appropriate personnel to implement the disaster recovery plan.
- The Disaster Recovery Plan shall be available if requested.

Data Backup Plan

RGV HIE shall work with its vendors on the following as defined by the HIPAA Security Rule:

- RGV HIE shall contractually require vendors to comply with HIPAA security rules for establishing a Data Backup Plan and shall verify that backup procedures are in place. RGV HIE may verify vendors' compliance through obtaining copies of certifications or other industry practice analysis of HIPAA compliance with security rules.
- A Data Backup Plan shall be established to create and maintain retrievable exact copies of all ePHI.
- All media used for backing up ePHI is stored in a physically secure environment, such as a secure, off-site storage facility or, if backup media remains on site, in a physically secure location, different from the location of the computer systems it backed up.
- If an off-site storage facility or backup service is used, a Business Associate Agreement must be used to ensure that the Business Associate will safeguard the ePHI in an appropriate manner.
- The Data Backup Plan will address the frequency of backup, which shall be at least daily

Emergency Mode Operation Plan

RGV HIE shall identify roles and responsibilities and develop procedures to be implemented in the event of a disaster or emergency in order to identify whether any critical information and or systems have been interrupted or negatively impacted, the degree of the impact and the actions required for restoration. RGV HIE shall periodically test the plan.

RGV HIE shall identify individuals or entities to be notified in the event of a disaster or emergency situation. Notification procedures shall address immediate actions as well as ongoing actions should the situation result in an extended period of interruption of service.

RGV HIE shall work with its technology vendors hosting ePHI to establish the following:

- Procedures to notify RGV HIE in the event of a disaster or emergency situation, including but not limited to: if PHI needs to be stored or moved, arrangements for transfer such as, where, when and by whom; and status updates.
- Procedures to continue critical business processes.

- Procedures for the protection and security of ePHI while operating in emergency mode.
- Procedures for retrieval of backup data.
- Emergency Mode Operation Plan shall be available if requested.

Testing and Revision Procedures

RGV HIE shall work with vendors hosting ePHI to review tests annually. Based on the review of responses during the test and the associated evaluation of those responses, revisions in the procedures may be made to ensure the organization has taken appropriate precautionary steps to protect critical functions.

- Data backup procedures shall be tested on a periodic basis to ensure that exact copies of ePHI can be retrieved and made available and results communicated to RGV HIE.
- Disaster recovery procedures shall be tested on a periodic basis to ensure that ePHI and the systems needed to make ePHI available can be restored or recovered and results communicated to RGV HIE.
- Emergency mode operation procedures shall be tested on a periodic basis to ensure that critical business processes can continue in a satisfactory manner while operating in emergency mode

Should an emergency or disaster actually occur, the individual overseeing the response at the specific location shall complete a summary of the following:

- Description of emergency situation, the various steps taken in the response process (notification, site assessment, restoration capability, operational capability and contingency actions)
- Problems that were encountered.
- Failures within the system to retrieve back-up information, adequacy of the procedures, lack of preparedness/training.
- After action review and recommendations for changes in policies and or procedures.

This summary shall be completed within 90 days of the event and forwarded to the RGV HIE Executive Director for review and possible changes in policies and procedures. The Executive Director will report recommendations for changes to the RGV HIE Board of Directors.

Key Functions Criticality Analysis

The importance of the system or part of the system to the overall operations and mission of the organization is the determining factor in its criticality. RGV HIE will work with its technology vendors to:

- Inventory key functions and assess the relative criticality of specific applications, components and data to prioritize business impact (ePHI, impact to RGV HIE employees and impact to clients).
- Analyze identified assets' recovery priority and time objective after an unplanned event

The assessment of data and application criticality shall be conducted periodically and at least annually to ensure that appropriate procedures are in place for data and applications at each level of risk.

RGV HIE shall work with vendors hosting ePHI to establish a Data Backup Plan, Disaster Recovery Plan and Emergency Mode Operation Plan.