RGVHIE Rio Grande Valley Health Information Exchange	Security	Rio Grande Valley HIE	Policy: S6
	Effective Date 11/20/2015	**Last Date Revised/Updated** 11/20/2015	**Date Board Approved:** 11/20/2015
Subject: **Administrative Safeguards - Information Access Management**			

FEDERAL REGULATION:
45 CFR 164.308(a)(4)

POLICY:

Rio Grande Valley Health Information Exchange (RGV HIE) has adopted this policy for authorized staff, employees and workforce to access RGV HIE information systems containing ePHI to provide protection for the use and disclosure of ePHI. This policy includes the following components:

- **Access authorization 164.308(a)(4)(ii)(B)**. RGV HIE shall implement procedures to authorize and/or restrict access to ePHI, including through workstation, laptop, transaction, program, process, and other tools and mechanisms.

- **Access establishment and modification 164.308(a)(4)(ii)(C)**. RGV HIE shall establish standards to document, review and modify access to RGV HIE systems.

In some cases, RGV HIE's technology vender is responsible for access requests from participating providers to systems managed by that vendor. In other cases, RGV HIE is responsible for all access requests from participating providers related to other systems. Also see the Service Agreements for provisions related to provider responsibilities for their authorized users, including the following:

- Provider agrees to provide RGV HIE with the name of an individual ["Superuser"] responsible for managing assignment and use of passwords by all individuals for whom Provider authorizes access. Provider agrees to provide the identifying information that RGV HIE requests about the Superuser to comply with HIPAA safeguards related to information access, such as name, job title, department, supervisor, and employee number or other identifier.

- Provider agrees to manage assignment and use of passwords and access to PHI as necessary and required to ensure compliance, including but not limited to deleting old users and adding new users within 2 Business days of the change in their user status. In addition, Provider agrees to require the Superuser to complete training and execute a document acknowledging responsibility for management of Provider's authorized users. Provider understands that the Superuser's responsibility for password management does not extend to authority to edit, amend, or change any data in the RGV HIE system.

- Provider agrees to provide information related to Superuser's management of authorized users on a regular basis as requested by RGV HIE to audit compliance by Superuser with this Agreement.

PROCEDURE:

ACCESS AUTHORIZATION

1. Access by RGV HIE Employees

The Executive Director or his designee shall grant access to staff, employees and workforce members to RGV HIE systems containing ePHI, including through workstation, laptop, transaction, program, process, and other tools and mechanisms and shall comply with RGV HIE Policy S5 Administrative Safeguards - Workforce Security. The Executive Director or his designee shall grant access using the System Access Request form and shall issue an individual user ID and assist the employee in constructing a confidential password for access to the system. *See RGV HIE Policy S15. Technical Safeguards - Access Controls*.

Access to systems containing ePHI: The Privacy Officer and Security Officer will determine standards to authorize or restrict access to RGV HIE systems containing or accessing ePHI in order to protect the confidentiality, integrity and availability of ePHI. The levels of access shall be based on legitimate need to perform job responsibilities.

Access to other systems: The Executive Director shall approve access and determine the access level to RGV HIE accounting, payroll and Human Resources software systems based on job functions and the need to access different aspects of RGV HIE's financial information.

Non-RGV HIE equipment: Employees using their own computer equipment to access the various operational programs and data within the RGV HIE network must:

- Receive approval from the Security and Privacy officers.
- Have their respective equipment approved for use by the Executive Director or his designee. *See HIPAA Policy S12. Physical Safeguards - Workstation Use.*

RGV HIE does not allow access to the network from a remote site.

Transfer of employees: The Executive Director shall review the access of, and modify as appropriate, any current employee transferring to a new job position or location within RGV HIE.

2. Access by Participating Provider or Other Outside Entities

Provider and Other Outside User Access: Requests for outside user access shall comply with the requirements in the Services Agreement and include:

- User Request form
- Identify the information systems containing ePHI.
- Name, position and location of individual.
- Purpose of access and level of access requested.
- Preferred start date and length of time access is requested.
- Confirmation of security training.

Vendor Access: Vendors requiring access to the RGV HIE network must contact the Executive Director in advance of their visit to RGV HIE. The Executive Director or his designee will provide access only for that period of time required for completion of the vendor's work. RGV HIE staff whose hardware or software requires vendor maintenance, repair, etc. must notify the Executive Director of the need for vendor service at the time the vendor is notified.

All vendors accessing ePHI through one of RGV HIE's programs must sign in or leave documentation indicating the date and time of service as well as the programs accessed and the work performed. Vendors must utilize their own passwords and unique identification to access their respective software programs. A log will be maintained which shall document the dates and times of vendor access.

Visitor Access: Visitors shall not have access to RGV HIE laptops, software programs databases or other RGV HIE systems that contain or access ePHI.

ACCESS ESTABLISHMENT AND MODIFICATION

The Executive Director shall document, review and modify (if needed) employee access to RGV HIE systems that contain ePHI at least annually. Review shall include:

- Date of review and estimated schedule for next review.
- Review of current access.
- Confirmation access is legitimate to accomplish job responsibilities.
- Confirmation of compliance with RGV HIE Policy S5 Administrative Safeguard - Workforce Security.
- Modification or restriction of access as necessary documenting on System Access Request form.

VIOLATIONS

Any individual, found to have violated this policy, may be subject to disciplinary action up to and including termination of employment.